高职高专计算机任务驱动模式教材

网络管理技术

李学祥 主编　　田挺 副主编



清华大学出版社

高职高专计算机任务驱动模式教材

网络管理技术

李学祥　主编
田　挺　副主编

清华大学出版社
北　京

内容简介

本教材是以教育部关于构建“以工作过程为导向”的课程体系、开发“工学结合”特色教材为设计思路，以一个职业人成长的经历为项目背景，按照基于工作过程的思路，通过简单网络设备配置与管理、局域网中的广播流量管理、局域网间互联、网络安全配置、无线网络配置、网络综合配置应用6个学习情境，全面讲述了局域网络中基于设备的主要管理与配置方法。书中配有大量插图和操作代码，内容充实，可操作性强。

本书可作为高职高专院校计算机专业、网络技术专业的教材，也可作为计算机网络公司工程技术人员的参考书。

图书在版编目（CIP）数据

网络管理技术/李学祥主编. —北京：清华大学出版社，2010.3
高职高专计算机任务驱动模式教材
ISBN 978-7-302-21909-5

Ⅰ. ①网…　Ⅱ. ①李…　Ⅲ. ①计算机网络－管理－高等学校：技术学校－教材
Ⅳ. ①TP393.07

中国版本图书馆 CIP 数据核字(2010)第 015901 号

责任编辑：束传政
责任校对：袁　芳
责任印制：李红英

出版发行：清华大学出版社　　**地　址：**北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　编：**100084
社 总 机：010-62770175　　**邮　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：清华大学印刷厂
经　销：全国新华书店
开　本：185×260　　**印　张：**12.5　　**字　数：**282 千字
版　次：2010 年 3 月第 1 版　　**印　次：**2010 年 3 月第 1 次印刷
印　数：1～3000
定　价：20.00 元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。联系电话：010-62770177 转 3103　　产品编号：030016-01

编审委员会

出版说明

我国高职高专教育经过近十年的发展，已经转向深度教学改革阶段。教育部2006年12月发布了教高[2006]16号文件“关于全面提高高等职业教育教学质量的若干意见”，大力推行工学结合，突出实践能力培养，全面提高高职高专教学质量。

清华大学出版社作为国内大学出版社的领跑者，为了进一步推动高职高专计算机专业教材的建设工作，适应高职高专院校计算机类人才培养的发展趋势，根据教高[2006]16号文件的精神，2007年秋季开始了切合新一轮教学改革的教材建设工作。

目前国内高职高专院校计算机网络与软件专业的教材品种繁多，但切合国家计算机网络与软件技术专业领域技能型紧缺人才培养培训方案并符合企业的实际需要、能够成体系的教材还不成熟。

我们组织国内对计算机网络和软件人才培养模式有研究并且有过一段实践经验的高职高专院校，进行了较长时间的研讨和调研，遴选出一批富有工程实践经验和教学经验的双师型教师，合力编写了这套适用于高职高专计算机网络、软件专业的教材。

本套教材的编写方法是以任务驱动案例教学为核心，以项目开发为主线。我们研究分析了国内外先进职业教育的培训模式、教学方法和教材特色，消化吸收优秀的经验和成果。以培养技术应用型人才为目标，以企业对人才的需要为依据，把软件工程和项目管理的思想完全融入教材体系，将基本技能培养和主流技术相结合，课程设置中重点突出、主辅分明、结构合理、衔接紧凑。教材侧重培养学生的实战操作能力，学、思、练相结合，旨在通过项目实践，增强学生的职业能力，使知识从书本中释放并转化为专业技能。

一、教材编写思想

本套教材以案例为中心，以技能培养为目标，围绕开发项目所用到知识点进行讲解，对某些知识点附上相关的例题，以帮助读者理解，进而将知识转变为技能。

考虑到是以“项目设计”为核心组织教学，所以在每一学期配有相应

的实训课程及项目开发手册，要求学生在教师的指导下，能整合本学期所学的知识内容，相互协作，综合应用该学期的知识进行项目开发。同时在教材中采用了大量的案例，这些案例紧密地结合教材中的各个知识点，循序渐进，由浅入深，在整体上体现了内容主导、实例解析，以点带面的模式，配合课程后期以项目设计贯穿教学内容的教学模式。

软件开发技术具有种类繁多、更新速度快的特点。本套教材在介绍软件开发主流技术的同时，帮助学生建立软件相关技术的横向及纵向的关系，培养学生综合应用所学知识的能力。

二、丛书特色

本系列教材体现目前的工学结合教改思想，充分结合教改现状，突出项目面向教学和任务驱动模式教学改革成果，打造立体化精品教材。

1. 参照或吸纳国内外优秀计算机网络、软件专业教材的编写思想，采用本土化的实际项目或者任务，以保证其有更强的实用性，并与理论内容有很强的关联性。

2. 准确把握高职高专软件专业人才的培养目标和特点。

3. 充分调查研究国内软件企业，确定了基于 Java 和.NET 的两个主流技术路线，再将其组合成相应的课程链。

4. 教材通过一个个的教学任务或者教学项目，在做中学，在学中做，以及边学边做，重点突出技能培养。在突出技能培养的同时，还介绍解决思路和方法，培养学生未来在就业岗位上的终身学习能力。

5. 借鉴或采用项目驱动的教学方法和考核制度，突出计算机网络、软件人才培训的先进性、工具性、实践性和应用性。

6. 以案例为中心，以能力培养为目标，并以实际工作的例子引入概念，符合学生的认知规律。语言简洁明了、清晰易懂、更具人性化。

7. 符合国家计算机网络、软件人才的培养目标；采用引入知识点、讲述知识点、强化知识点、应用知识点、综合知识点的模式，由浅入深地展开对技术内容的讲述。

8. 为了便于教师授课和学生学习，清华大学出版社正在建设本套教材的教学服务资源。在清华大学出版社网站(www.tup.com.cn)免费提供教材的电子课件、案例库等资源。

高职高专教育正处于新一轮教学深度改革时期，从专业设置、课程体系建设到教材建设，依然是新课题。希望各高职高专院校在教学实践中积极提出意见和建议，并及时反馈给我们。清华大学出版社将对已出版的教材不断地修订、完善，提高教材质量，完善教材服务体系，为我国的高职高专教育继续出版优秀的高质量的教材。

清华大学出版社

高职高专计算机任务驱动模式教材编审委员会

rawstone@126.com

2009 年 1 月 1 日

前　言

2006 年，教育部、财政部联合推行国家示范性高职院校建设项目，提出以专业建设为核心，以创新“工学结合”人才培养模式为改革切入点，通过三年的时间，在全国建设 100 所示范性高职院校，在区域乃至全国起到辐射带动作用。在示范院校建设项目中，明确了创新“工学结合”人才培养模式和“以工作过程为导向”的课程体系两个核心建设点。其中，开发“工学结合”的特色教材是课程建设中的核心内容。因而，应该把“工学结合”的思想和基于工作过程的思路深入到教材开发和设计的方方面面，以此推动专业建设与发展，进而培养符合区域经济发展需求的高技能人才。

本书就是为了示范专业建设需要而开发的特色创新教材。本教材以一个职业人的成长为主线，以任务驱动为编写体例，按照基于工作过程的教学思想来设计和开发教学与实践内容。通过本教材的学习和实践，再参考其他相关书籍，即使是刚刚接触网络的用户，也可以独立地完成网络的规划和构建工作。

本教材共分为 6 个情境，分别如下：

学习情境 1　简单网络设备配置与管理；

学习情境 2　局域网中的广播流量管理；

学习情境 3　局域网间互联；

学习情境 4　网络安全配置；

学习情境 5　无线网络配置；

学习情境 6　网络综合配置应用。

本书具有如下一些特色和价值：

(1) 按照职业成长历程来规划设计教学情境，按阶梯递进式“由易到难，由简单到复杂”地构建学习情境，使得学生在学习过程中体验“职业人”成长的历程。

(2) 基于工作过程的教学思想，通过资讯→决策→计划→实施→检查→评估 6 个环节，实现“教学做一体化”的教材设计目标。

(3) 采用“知识性与技能性相结合”的模式，体现理论的适度性、实践的指导性、应用的完整性。

(4) 按照知识够用的原则，将知识点贯穿于任务实施的过程中，层次清晰，概念简洁，叙述清楚，图文并茂，操作性强。

本教材由淄博职业学院信息工程系的李学祥任主编，田挺任副主编，同时参与编写的还有张志浩、郑保强、蔡可追等。其中，学习情境1由郑保强编写，学习情境2和学习情境6由田挺编写，学习情境3由李学祥编写，学习情境4由蔡可追编写，学习情境5由张志浩编写，在本教材的编写过程中还得到思科、锐捷等网络公司相关工程技术人员的指导和帮助，在此表示衷心的感谢。

由于编者学识有限，所以书中难免有不妥和错误之处，恳请广大读者批评指正。

编 者

2009年10月

目　录

学习情境 1　简单网络设备配置与管理

任务情境(资讯)

计算机网络近年来发展迅速。20 年前,在我国很少有人接触过网络。现在,计算机网络以及 Internet 已成为我们社会结构的一个基本组成部分。网络被广泛应用于工商业社会生活的各个方面,包括电子银行、电子商务、现代化的企业管理、信息服务等都以计算机网络系统为基础。从学校远程教育到政府日常办公,乃至现在的电子社区,很多方面都离不开网络技术。可以不夸张地说,网络在当今世界无处不在。

网络的飞速发展需要配套的网络管理,所以了解和掌握网络,特别是简单网络的配置与管理成为我们的必修课。网络是现代的信息基础设施,人们需要的信息传递、营销、服务、交流、娱乐等各种活动都可以通过网络完成,网络的质量直接决定了社会生活和经济生活的质量。在计算机网络的质量体系中,网络管理是一个关键环节,网络管理的质量直接影响网络的运行质量。

从广义上讲,任何一个系统都需要管理,只是由于系统的大小、复杂性的不同,管理在整个系统中的重要性也就有重有轻。网络也是一个系统。虽然网络管理很早就有,却一直没有得到应有的重视。这是因为以前的网络规模较小,而且复杂性不高,简单的网络管理系统就可以满足网络正常运行的需要,因而对其研究较少。但随着网络的发展,其规模逐渐增大,复杂性增加,网络管理技术凸显其重要性,而网络正常的运行对于网络管理的依赖性也越来越大。

任务分析(决策)

1. 计算机网络的概念

所谓计算机网络,就是将分散的计算机通过通信线路有机地结合在一起,形成相互通信、软/硬件资源共享的综合系统。

网络是计算机的一个群体,是由多台计算机组成的,这些计算机通过一定的通信介质互联在一起。计算机之间的互联,是指彼此之间能够交换信息。互联通常有两种方式:即计算机间通过双绞线、同轴电缆、电话线、光纤等有形通信介质连接,或通过激光、微波、地球卫星通信信道等无形介质互联。

随着计算机技术的迅猛发展,计算机的应用逐渐渗透到各个技术领域和社会生活的各个方面。社会的信息化、数据的分布处理、计算机资源的共享等各种应用要求推动计算机技术朝着群体化方向发展,促使计算机技术与通信技术紧密结合。计算机网络属于多

机系统的范畴，是计算机和通信这两大现代技术相结合的产物，它代表着当前计算机体系结构发展的一个重要方向。

计算机网络通常分为3大类：多机系统、局域网(LAN)和广域网(WAN)(或称远程网络)。以微机为主组成的局域网是当今计算机应用中的一个空前活跃的领域。局域网技术从20世纪60年代开始萌芽，经过20世纪70年代的大发展，20世纪80年代走向成熟。到了20世纪90年代，局域网技术更趋于成熟，光纤开始发展，局域网应用大量普及。

2. 什么是网络管理

按照国际标准化组织(ISO)的定义，网络管理是指规划、监督、控制网络资源的使用和网络的各种活动，以使网络的性能达到最优。网络管理的目的在于提供对计算机网络进行规划、设计、操作运行、管理、监视、分析、控制、评估和扩展的手段，从而合理地组织和利用系统资源，提供安全、可靠、有效和友好的服务。

简单地讲，网络管理就是通过某种方式对网络状态进行调整，使网络能正常、高效地运行。其目的很明确，就是使网络中的各种资源得到更加高效的利用；当网络出现故障时，能及时做出报告和处理，并协调、保持网络的高效运行。

3. 网络管理的分类及功能是怎样的

根据国际标准化组织的定义，网络管理有5大功能：故障管理、配置管理、性能管理、安全管理及计费管理。

(1) 网络故障管理

计算机网络出现意外故障是常有的事情，在很多情况下，故障的发生可能对网络的使用者带来难以估价的损失。由于发生失效故障时，往往不能迅速、有效地确定故障所在的准确位置，而需要相关技术的支持，因此，需要有一个故障管理系统来检测、定位和排除网络硬件和软件中的故障。当出现故障时，该功能能确认并记录故障，找出其位置并尽可能排除它，保证网络能提供连续、可靠的服务。

(2) 网络配置管理

一个实际中使用的计算机网络是由多个厂家提供的产品、设备相互连接而成的，因此各设备需要相互了解和适应与其发生关系的其他设备的参数、状态等信息，否则就不能有效甚至正常地工作。尤其是网络系统常常是动态变化的，如网络系统本身要随着用户的增减、设备的维修或更新来调整网络配置，因此需要有足够的技术手段支持这种调整或改变，使网络能更有效地工作。另外，要掌握和控制网络的状态，包括网络内各个设备的状态及其连接关系。网络配置管理的典型方法是用逻辑图来描绘所有网络设备及其逻辑关系，并将网络的确切物理布局以适当的比例映射到这个逻辑图上；还要用精心设计的图标来表示各种网络对象，图标涂上不同颜色表示设备的不同状态。

(3) 网络性能管理

鉴于网络资源的有限性，最理想的情况是在占用最少的网络资源和支出最少通信费用的前提下，网络提供持续、可靠的通信能力，并使网络资源得到最有效的利用。这主要

考察网络运行状态的好坏。网络性能管理使网络管理员能够监视网络运行的参数，如吞吐量、响应时间及网络的可用性等。

(4) 网络安全管理

计算机网络系统的特点决定了网络安全固有的脆弱性，要确保网络资源不被非法使用，确保网络管理系统本身不被未经授权的访问，保持网络管理信息的机密性和完整性。网络安全管理是对网络资源及其重要信息访问的约束和控制，包括验证网络用户的访问权限和优先级，检测和记录未授权用户企图进行的不应有的操作。

(5) 网络计费管理

在有偿使用计算机网络系统中的信息资源的情况下，需要能够记录和统计哪些用户利用哪条通信线路传输了多少信息，以及完成什么工作等。在非商业化的网络上，仍然需要统计各条线路工作的繁闲情况和不同资源的利用情况，以供决策参考。账务计费管理提供了计算一个特定网络或网段的运行成本的手段，以度量各个用户和应用程序对网络资源的使用情况。

任务设计(计划)

任务 1.1　熟悉网络设备操作系统
任务 1.2　连接网络设备
任务 1.3　IP 地址分配及 IP 子网划分

任务实施(实施)

任务 1.1　熟悉网络设备操作系统

下面以 Cisco 系列产品的 IOS 来介绍网络设备操作系统的概念。

1.1.1　简单了解设备及连接

网络互联主要是通过局域网和广域网来实现的，连接局域网和广域网使用的设备和技术完全不同。下面主要介绍网络设备在局域网和广域网中的连接方法。

1. 直连线

直连线的特点是一根电缆的两头的接线顺序完全一致，即一端为 568 B，另一端也为 568 B；或者一端为 568 A，另一端也为 568 A；这保证了接到 RJ 45 头的同一根针的线的两个末端完全一样。可以用下面的方法来检查是否为直连线：把同一根线上的两个 RJ 45 头按照同一个方向摆在一起，其连线的顺序是一样的。

直连线大多用于不同层设备的连接，但也有例外。采用直连线的有：

① 交换机和路由器相连；

② 交换机和 PC 机或服务器相连；

③ 集线器和 PC 机或服务器相连。

还有一种方法判断是否采用直连线：在连接设备时，查看设备的端口下面是否有一个“X”标志。如果要连接的两个设备的端口一个有“X”，而另一个没有“X”，则使用的是直连线。

2. 交叉线

交叉线的特点是在一根电缆的两端，其接线顺序一端为 568 A，另一端为 568 B。这样相当于一端的第一根针和另一端的第三根针连在一起；一端的第二根针和另一端的第六根针连在一起。这样做的目的是为了适当地校正、传递和接收设备信号。

交叉线大多用于相同设备的连接，但也有例外。采用交叉线的有：

① 交换机和交换机相连；

② 集线器和集线器相连；

③ 路由器和路由器相连；

④ PC 和 PC 相连；

⑤ 交换机和集线器相连。

3. 翻转线

翻转线正好和直连线相反，即一根电缆的两端线序完全相反，即把同一根线的两个 RJ-45 头按照同一个方向摆在一起，其线序是完全相反的。

翻转线只用于一种情况，即始终和 Cisco 设备的控制台(Console)端口的连接。

1.1.2 操作系统简介

互联网操作系统(IOS，Internetwork Operating System)是由 Cisco 公司开发的用于管理 Cisco 网络设备的操作系统。Cisco 公司的很多网络设备都使用 IOS，其最新版本是 12.3。

使用 IOS 软件最常用的方法是通过 IOS 的命令行接口(CLI，Command Line Interface)。通过管理控制台端口、AUX(Modem 连接)或者 Telnet，都可以进行 IOS CLI 的配置。对 IOS 命令行接口的访问也称为 Exec 会话。IOS 的 CLI 是一种类 DOS 的界面，用户通过输入相应的命令来配置 IOS，除了密码外，IOS 命令不区分大小写。

1. Cisco 设备的启动

在了解 IOS 之前，有必要先对 Cisco 设备的工作方式有所了解，包括 Cisco 设备的启动过程、配置方式等等。

不管是 Cisco 的路由器还是交换机，它们的启动都有以下过程：

① 发现和检测硬件设备(包括设备内部的各种组件)；

② 发现和安装 IOS 软件；

③ 发现和应用配置文件。

这里介绍的启动过程只是一个概述，后面的章节将详细介绍这些过程。

2. 设备的配置方法

配置 Cisco 设备的方法有以下几种：

① 通过控制台端口配置：其优点是配置简单；缺点是不能进行远程配置，并且安全性也不高。

② 通过 AUX(auxiliary)口配置：在路由器的背面有一个 AUX 口，通过它可以进行远程配置，把 AUX 口与 Modem 相连，管理员就可以通过远程网络拨号到这个 Modem 进行过程控制了。

③ 通过虚拟终端(Virtual Terminal)配置：配置 Cisco 设备的一种常用方法是通过 Telnet 来配置。在某个终端设备中运行 Telnet 应用程序来进行远程控制，就像在本地控制一样。在使用 Telnet 之前，必须在被控制的设备上配置 IP 地址，确保该设备能在网络工作。这种配置方式的优点是方便、安全。由于路由器等网络设备在网络中都是关键的设备，因此通常都集中放在某个机房，并且要上锁保护，网络管理员可以在不进入机房的情况下通过 Telnet 远程配置路由器。但这种安全性也是相对的，因为如果网络管理员的密码泄露，那么人人都可以控制路由器了。另外，对于刚出厂的设备(没有任何配置)时，不能使用 Telnet。

④ 通过 TFTP 服务器配置：TFTP 服务器是一台 PC 或者 UNIX 服务器。它可以用于备份 Cisco 设备的配置文件，可以通过从 TFTP 服务器上下载配置文件来配置 Cisco 设备。当然，前提是要配置的设备必须有一些基本配置，能在网络中工作。

作为网络管理人员，要配置 Cisco 的网络设备，通常采用下述方式：对于刚买的设备(没有任何配置)，通过控制台端口来配置；对该设备进行完成基本配置后，该设备已经能够在网络中工作了。要进行更深入的 Telnet 配置，可采用 Telnet 或其他远程配置方式来配置。

3. 用户模式和特权模式

要配置 Cisco 路由器，必须首先登录到该路由器，之后才能输入命令。登录可以是远程登录的，或是通过一个终端使用路由器的用户界面来登录。

出于安全的考虑，路由器有两级的命令访问控制：用户模式和特权模式。

特权模式的提示符是："路由器名称 + 英镑符号(#)"，由此可以确定用户处于特权 Exec 模式。在这个级别上，用户可以完全访问路由器。在特权 Exec 模式中，可使用所有的命令，包括在用户 Exec 模式中使用的基本的故障排除和状态检查命令，以及修改路由器配置的命令，执行可能破坏网络的测试，重新启动路由器和查看配置文件。

要退出特权 Exec 模式并回到用户 Exec 模式，可使用命令 disable。

表1-1列出了进入和退出用户模式与特权模式的命令。

表 1-1　进入和退出用户模式与特权模式的命令列表

命　　令	说　　明
Router>enable	用户模式下的命令，用于进入特权模式，可以简写为 en
Router>exit(logout,quit)	从用户模式退回到 Exec 模式
Router # disable	从特权模式退回到用户模式
Router # exit(logout,quit)	从特权模式退回到 Exec 模式

注意表 1-1 中的 exit，logout 和 quit 命令。exit 用于从下一级子菜单返回到上一级子菜单，在其他模式也是可用的；logout 和 quit 命令，只用在用户模式或特权模式。为学习方便，本书在讲命令时，命令前的提示符也一并列出。

另外，特权模式也是进入其他模式的基础，也就是说，必须先进入特权模式，才能进入路由器的其他模式。

4. 其他配置模式

从特权模式可以进入全局配置模式（Global Configuration），在全局配置模式下可以进一步访问其他特殊的模式。

从特权模式进入全局配置模式的命令为：

```
(提示符 Routerb# 下)config terminal
```

全局配置模式的提示符为：

```
Routerb(config)#
```

在全局配置模式下可以进入其他特殊模式，如接口模式、子接口模式和链路模式。其中，链路模式有如下两种情况：

(1) 用于配置控制台端口的参数

进入链路模式的命令为：

```
Router(config)# line console 0
```

它的提示符为：

```
Router(config-line)#
```

(2) 用于 Telnet 进行远程登录

路由器有 5 条 VTY（Virtual Teletypes terminals，虚拟远程终端）链路（0～4），路由器允许存在并发的远程登录连接，也就是说，可以同时有 5 个 Telnet 会话连接到路由器。可以配置 VTY 的一条链路，或者一次对这 5 条链路同时配置。由于一个 Telnet 会话会随机选用一条 VTY，所以一般会对 5 条链路同时配置。

进入链路模式的命令为：

```
Routerb(config)# line vty  第一条 VTY 的编号  最后一条 VTY 的编号
```

例如：

```
Routerb(config)#line vty 04
```

5. 路由器的 Setup 模式

Setup 模式是路由器的一种特殊模式，其主要目的是为那些找不到配置的路由器提供最小化配置。在 Setup 模式中可以完成大部分的路由器配置，当然，这些配置也可以通过输入相应的命令来完成。当第一次启动路由器(路由器没有进行任何配置时)时，就会自动进入 Setup 模式，也可以在特权模式下输入"Setup"进入该模式。

路由器没有任何默认配置，当把配置文件删除时，就会进入 Setup 模式。交换机则不同，交换机有一个出厂的默认配置，当把交换机的配置文件删除时，就会返回默认配置。

6. 配置路由器的简单命令

① show：用于查看路由器的状态，其功能和交换机中的类似。
② show version：显示路由器的硬件配置、软件版本和 IOS 文件名等信息。
③ show running-config：显示当前 RAM 中的信息。
④ show startup-config：显示 NVRAM 的信息。

任何当前的配置都存储在 RAM 中。如果不保存，重新启动路由器时，以前的配置就会丢失。如果使用保存命令，会把当前的配置保存到 NVRAM 里，断电时就不会丢失。同样，也可以把 NVRAM 里的配置信息复制到 RAM 中来。Setup 模式的配置会同时写入到 RAM 和 NVRAM 中，相关命令如表 1-2 所示。

表 1-2　RAM 与 NVRAM 互相写入的命令

命　　令	说　　明
Router # copy running-config startup-config	把配置信息从 RAM 写入到 NVRAM
Router # copy startup-config running-config	把配置信息从 NVRAM 写入到 RAM
Router # write erase	清空 NVRAM 的配置，重启后进入 Setup 模式

7. 配置密码

由于路由器是关键的网络设备，因此其安全性是很重要的问题。密码是防止非法访问的一种常用方法。密码的应用有很多种，在这里主要介绍进入特权模式密码、控制台端口管理密码和 Telnet 密码。

(1) 特权模式密码

我们知道，从用户模式进入特权模式要输入密码，这个密码通过表 1-3 中的命令来配置。

表 1-3　特权模式密码的配置命令

命　　令	说　　明
Router(config) # enable password 密码字符串	配置明文密码(password 密码)
Router(config) # enable secret 密码字符串	配置密文密码(secret 密码)

注意：password 和 secret 密码都是用于进入特权模式的密码。password 密码没有 secret 密码安全，因为使用 show running config 命令查看配置时，password 密码会以明文形式显示出来，而 secret 密码则显示为乱码。另外，如果 password 和 secret 密码都配置且两者不相同(系统不允许相同)，会以 secret 密码为准。

(2) 控制台端口管理密码

该密码用于控制通过控制台端口访问的路由器，也就是说，用户必须输入控制台端口管理密码，才能通过控制台端口访问路由器。

配置控制台端口管理密码的步骤如下：

① 在全局配置模式下(即在"Router(config)#"下)输入"line consol 0"，然后按 Enter 键。该命令用于进入配置控制台端口参数的链路模式。

② 在提示符"Router(config-line)#"下输入"login"，然后按 Enter 键。

③ 在提示符"Router(config-line)#"下输入"password 密码字符串"，然后按 Enter 键。

(3) Telnet 密码

还有一种密码称为 VTY 密码。VTY 密码主要用于控制 Telnet 的访问，若希望通过 Telnet 来远程访问路由器，必须输入此密码。

VTY 密码的配置步骤如下：

① 在提示符"Router(config)#"下输入"line vty 0 4"，然后按 Enter 键。注意，由于 Telnet 会随即选择一条 VTY，所以要对全部的 5 条 VTY 都进行配置。

② 在提示符"Router(config-line)#"下输入"login"，然后按 Enter 键。

③ 在提示符"Router(config-line)#"下输入"password 密码字符串"，然后按 Enter 键。

8. 配置文件的管理

路由器的 RAM 类似 PC 上的内存，当前的配置都存储在 RAM 中。如果不保存，路由器重新启动后，RAM 的内容就会丢失，因此需要把 RAM 中的内容保存到 NVRAM 中，NVRAW 的内容在路由器重新启动时不会丢失。

通过控制台端口配置的信息都存储在 RAM 中。Setup 模式中的配置信息既写入到 RAM 中，又写入到 NVRAM 中。RAM 和 NVRAM 的内容可以相互修改，其相关命令见表 1-4。

表 1-4　RAM 和 NVRAM 的相关命令

命　　令	说　　明
Router # show running config	查看 RAM 中的配置信息
Router # show startup-config	查看 NVRAM 中的配置信息
Router # copy running-config startup-config	把 RAM 中的信息保存到 NVRAM(2600 系列路由器也可用 write 命令)
Router # copy start-config running-config	把 NVRAM 信息调入 RAM 中
Router # write erase	清空 NVRAM,路由器重启后进入 Setup 模式

9. 配置接口的状态

当使用 show 命令查看接口时,会看到有这样的显示:"Ethernet 0/0 is up,line protocol is up"。"Ethernet 0/0 is×××"代表硬件接口,即物理层连接是否正常。"line protocol is×××"代表数据链路层连接是否正常。一共有以下 4 种情况:

① Ethernet 0/0 is up,line protocol is up:表明物理层和数据链路层连接都正常。

② Ethernet 0/0 is up,line protocol is down:表明物理层连接虽然正常,但数据链路层连接错误。

③ Ethernet 0/0 is down,line protocol is down:表明物理层连接错误,导致数据链路层连接措错误(物理层连接错误,则数据链路层连接一定错误),从而接口不能转发数据。

④ Ethernet 0/0 is administratively,line protocol is down:表明管理员手动关闭了某个接口,导致该接口不能转发数据。用于关闭和启用某个接口的命令见表 1-5。

表 1-5　关闭和启用某个接口

命　　令	说　　明
Router(config-if) # shutdown	关闭某个接口
Router(config-if) # no shutdown	重新启用某个接口

任务 1.2　连接网络设备

本任务主要以交换机为例来介绍设备的连接方法。

1.2.1　如何启动网络设备?

1. 加电前的安装与检查

在给交换机加电之前,应对交换机的安装做必要的检查,以确保如下事项:

① 交换机已安放牢固。

② 如果配有接口模块，需确认此模块已被正确安装。

③ 所有通信电缆和光缆连接正确。

④ 电源线和地线连接正确，且供电电压与交换机的要求一致。

⑤ 配置电缆连接正确，终端控制台已经打开并设置完毕。

⑥ 供电电压与交换机的要求一致。

2. 交换机加电

在严格按照以上第一步的要求步骤完成交换机的安装和检查之后，就可以给交换机加电了。加电的顺序应该是首先打开供电电源的开关，然后打开交换机的电源开关。

3. 加电后交换机各指示灯状态

给交换机加电后，交换机前面板上的LED状态指示灯将出现如下反应：

① 交换机刚刚加电时，POWER和SYSTEM指示灯点亮，所有端口的LED指示灯快速闪亮，表示系统正在进行复位。

② 交换机完成自检并成功加载系统软件后进入正常工作状态，此时SYSTEM指示灯闪烁；对于已有可靠连接的接口，其LINK指示灯长亮。当接口有数据收发时，ACT指示灯闪烁或长亮；当没有数据收发时，ACT指示灯为暗。

③ 如果加电之前Console口上连接了PC，已经正确配置并启动了超级终端软件，则在系统通电后，屏幕上将出现公司名称、产品序列号及软、硬件版本等产品信息，并在自检完成后出现操作提示。按Enter键进入系统登录状态，输入用户名称和相应的密码后进入交换机的用户配置模式，进行相应的操作。

1.2.2 配置网络设备的途径有哪些？

可采用如下三种方法实现对交换机的配置管理：

① 通过串口控制台配置交换机；

② 通过Telnet配置交换机；

③ 通过SNMP管理交换机。

1. 通过串口控制台配置交换机

配置终端可以是一台PC，利用一条配置电缆，将其一端的DB9接头与PC的一个串口连接，将另一端的RJ-45接头与交换机的Console口连接。

2. 通过Telnet配置交换机

通过Telnet可实现对交换机的远程配置管理。在使用Telnet前，需要首先通过控制台端口配置交换机的IP地址和子网掩码。实现Telnet配置交换机的网络连接图如

图1 1所示，其中，PC1通过局域网与交换机相连；PC2作为终端控制台通过配置电缆连接到交换机的Console口，用以配置交换机的IP地址。

例如，此时PC1的IP地址为192.168.0.3/24，若想通过PC1以Telnet方式管理交换机，请按照以下步骤进行配置。

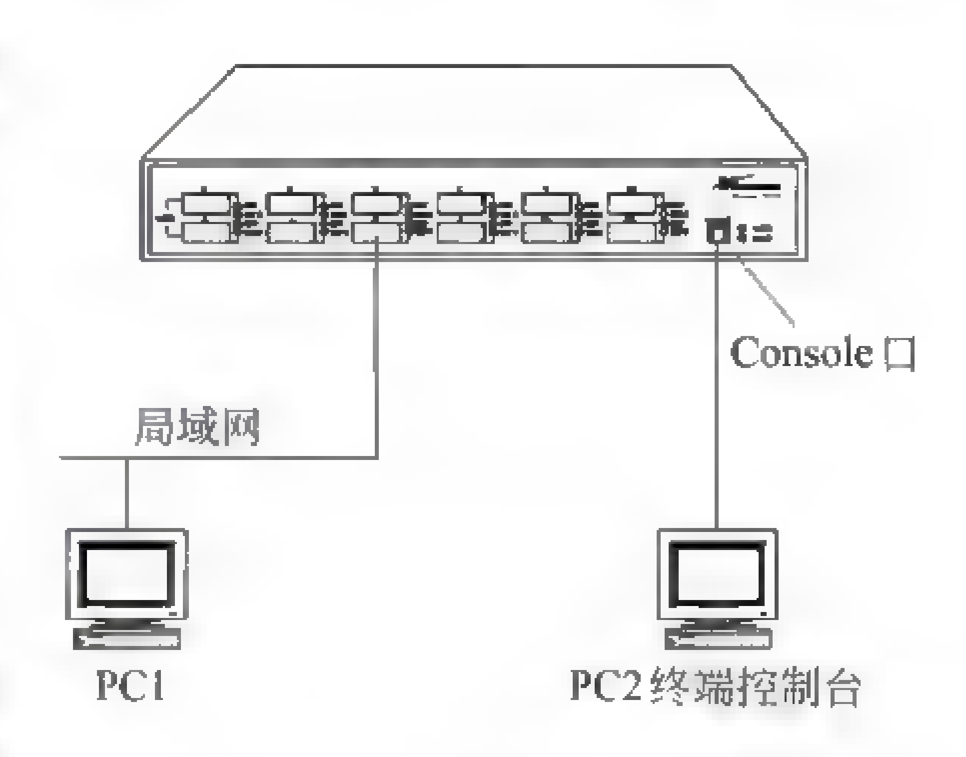


图1 1 实现Telnet配置交换机的网络连接图

步骤1：为交换机配置IP地址。

PC2通过配置电缆与交换机的Console口连接，然后在PC2终端控制台上使用以下命令配置交换机的IP地址(设地址为192.168.0.1/24)：

```
Switch(config)#interface vlan default
Switch(config-vlan-default)# ip address 192.168.0.1/24
```

注意：交换机的IP地址一定与PC1的IP地址在同一网段(本例中，PC1的IP地址为192.168.0.0/24)。

步骤2：使能Telnet服务。

在出厂默认状态下，交换机的Telnet服务功能是打开的，如果你已经关闭了该服务功能，请用以下命令使能Telnet服务：

```
Switch(config)#service telnet enable
```

步骤3：利用Telnet登录交换机。

在PC1上运行Telnet程序，输入命令"telnet 192.168.0.3"，单击"确定"按钮后进入登录页面，输入正确的用户名和密码后即可实现对交换机的配置管理。

3. 通过SNMP管理交换机

如果交换机支持使用SNMP协议管理，用户必须先在用于管理交换机的PC上安装网管软件(该网管软件可以从供应商或者代理商处获得)。组网方法如图1-1所示，操作方法步骤如下：

步骤1：通过PC2配置default vlan的IP地址。

```
Switch(config)#interface vlan default
Switch(config-vlan-default)#ip address 192.168.0.1/24
```

步骤2：打开SNMP服务功能。在交换机的出厂默认状态下，SNMP服务功能是关闭的，请用以下命令打开该服务功能：

```
Switch(config)#service snmp enable
```

步骤3：启动网管软件，登录交换机。在启动了网管软件之后，首先要进行用户登录，用户登录成功后可以配置设备。

任务 1.3 IP 地址分配及 IP 子网划分

对于网络管理来讲，IP 地址都是一个十分重要的概念，Internet 的许多服务和特点都是由 IP 地址体现出来的，而 IP 地址和子网掩码的设置，更是从事网络工作的人必须具备的网络基础知识，只有理解了 IP 地址和子网掩码的真正含义，才能得心应手地管理一个网络。我们要想理解 IP 地址的真正应用，首先要了解 IP 地址与子网掩码的常识。

1.3.1 IP 地址概述

在网络中，我们需要唯一地标识 Internet 上的每一个设备，以确保所有设备全球通信。这好像在电话系统中，每一个电话用户都有唯一的电话号码一样(如果我们把国家码和地区码都看成是这个标志系统的一部分)。

Internet 协议地址(简称 IP 地址)对网上某个节点来说是一个逻辑地址，IP 是唯一的。地址唯一是指每一个地址定义了一个且仅有一个到 Internet 的连接。在 Internet 上的两个设备永远不会有相同的地址。但是，如果一个设备通过两个网络与 Internet 相连，那么这个设备就有两个 IP 地址。

1. 地址空间

IP 协议定义的地址具有地址空间。地址空间就是协议所使用的地址总数。如果协议使用 n 位来定义地址，那么地址空间就是 2^n，因为每一位可以有两种不同的值(1 或 0)。

现在采用的 IP 协议版本为 IPv4，它使用 32 位地址，这表示地址空间是 2^{32}，或 4294967296(超过 40 亿)。这就表明，从理论上讲，可以有超过 40 亿个设备连接到 Internet。但实际的数字要远小于这个数值。

2. IP 地址的表示方法

IP 地址有三种常用的表示方法，即二进制表示法、点分十进制表示法和十六进制表示法。

(1) 二进制表示法

在二进制表示法中，IP 地址表现为 32 位。为了使这个地址有更好的可读性，通常在每个字节(8 位)之间加上一个或多个空格。这样，有时就会听到说：IP 地址是 32 位地址、4 个八位组地址，或者 4 字节地址。下面是二进制 IP 地址的示例：

01110101 10010101 00011101 11101010

(2) 点分十进制表示法

为了使 32 位地址更加简洁和更容易阅读，Internet 的地址通常写成小数点将各字节

分隔开的形式。如图1-2所示为用点分十进制表示的IP地址。应当注意到，因为每个字节仅有8位，因此在用点分十进制表示法表示的IP地址中，每个点分十进制数一定在0～255。

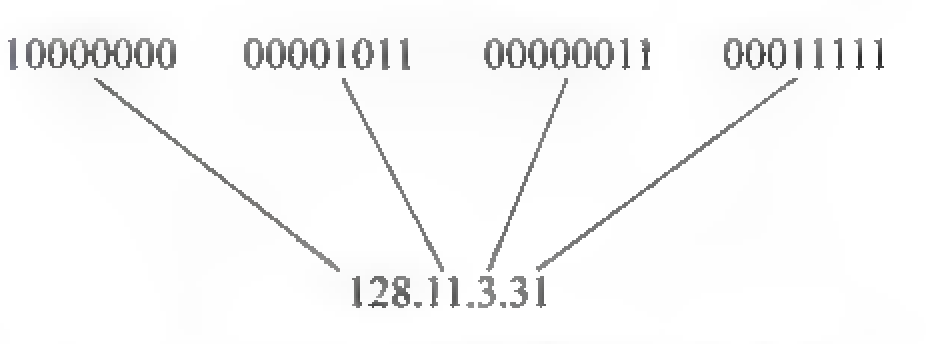


图1-2　用点分十进制表示的IP地址

(3) 十六进制表示法

有时我们会见到用十六进制数表示的IP地址。每一个十六进制数等价于四个4位。这就是说，一个32位的地址要用8个十六进制数字来表示。这种表示方法常用于网络编程中。例如，10000001 00001011 00001011 11100111 表示成十六进制数为0x819B0BEF。

3. IP地址的分类

在最初设计互联网时，为了便于寻址以及层次化构造网络，每个IP地址包括两部分，即网络号(Network ID)和主机号(Host ID)。同一个物理网络上的所有主机都使用同一个网络号，网络上的一个主机有一个主机号与其对应。

IP地址可分成五类，即A类、B类、C类、D类和E类。E类一般用于实验组网，日常组网中极少用到，在此不做详细描述。五类地址的组成结构如图1-3所示。每一类IP地址占据整个地址空间的某一部分。图1-4给出了每一类IP地址的空间占用情况(近似的)。

从图1-4可以看出，A类地址占据了整个地址空间的一半，这是设计中的缺陷。B类地址占据了整个地址空间的1/4，这也是一个缺陷。C类地址占据地址空间的1/8，而D类和E类地址各占据地址空间的1/16。表1-6给出了每一类IP地址的数量。



图1-3　IP地址分类

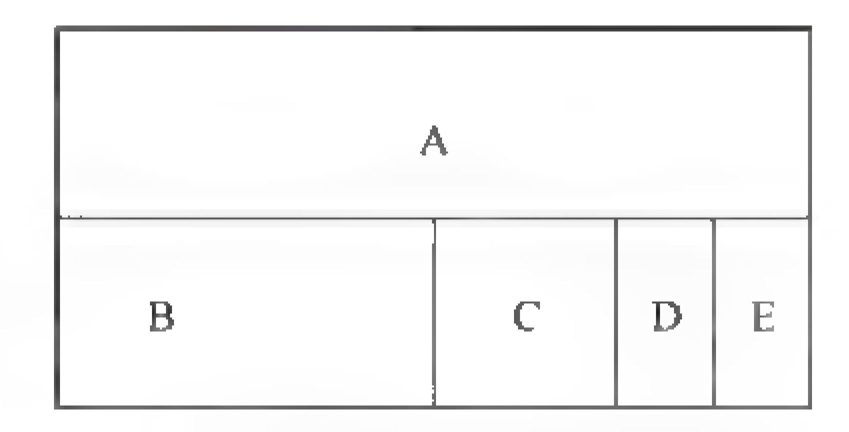


图1-4　地址空间占用情况

表1-6　每一类IP地址的数量及占地址空间的比例

类别	地址数量	占地址空间的比例/%
A	2^{31}=2147483648	50
B	2^{30}=1073741824	25
C	2^{29}=536870912	12.5
D	2^{28}=268435456	6.25
E	2^{28}=268435456	6.25

如图 1 3 所示，A 类地址的最高位 0 和随后的 7 位是网络号部分，剩下的 24 位表示网内主机号。在 一个互联网内可能会有 126 个 A 类网络(网络号 1～126，号码 0 和 127 保留)，而每 一个 A 类网络中允许有 1600 万个节点。对于非常大的地区网，如美国的 MLNET 和某些很大的商业网，才能使用 A 类地址。

B 类地址的最高两位 10 和随后的 14 位是网络号部分，剩下的 16 位表示网内的主机号。这样，在某种互联环境下可能有大约 16000 个 B 类网络，每个 B 类网络中可以有 65000 多个节点。一般大单位和大公司营建的网络使用 B 类地址。

C 类地址的最高位 110 和随后的 21 位是网络号部分，剩下的 8 位表示网内主机号。这样，一个互联网将允许包含 200 万个 C 类网络，每 一个 C 类网络中最多可以有 254 个节点。较小的单位和公司都使用 C 类地址。

D 类地址的最高 4 位为 1110，表示多播地址，即一个多播组的组号。

如果用户不喜欢使用二进制，也可以按照 IP 地址第 一字节值的十进制表示划分四类网络。A 类地址以 1～127 开始，B 类地址以 128～191 开始，C 类地址以 192～223 开始，D 类地址以 224～239 开始。

4. 网络掩码和默认掩码

网络掩码是一个 32 位数。当用掩码和地址段中的一个地址按位相“与”(AND)时，就可得出该地址段的第一个地址(网络地址)。

在网络掩码中，二进制值为 1 的位代表网络位，二进制值为 0 的位代表主机位。

A，B，C 三类地址中的默认子网掩码见表 1-7。

表 1-7　默认子网掩码

类	用二进制值表示的掩码	用点分十进制值表示的掩码
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

5. 特殊地址

A 类、B 类和 C 类地址中的某部分空间可用作特殊的地址(见表 1-8)。

表 1-8　特殊地址

特殊地址	网络位	主机位	源地址或目的地址
网络地址	特写的	全 0	都不是
直接广播地址	特写的	全 1	目的地址
受限广播地址	全 1	全 1	目的地址
环回地址	127	任意	目的地址

(1) 网络地址

A,B,C 类地址中的第一组定义了该主机所在的网络地址。例如,主机 123.50.16.90 所在的网络地址为 123.0.0.0;150.48.0.1 所在的网络地址为 150.0.0.0。

(2) 直接广播地址

在 A,B,C 类地址中,若主机位是全 1,则该地址称为直接广播地址。路由器使用这种地址把一个数据包发送到特定网络上的所有主机。所有的主机都会收到具有这种类型目的地址的数据包。这个地址在 IP 数据包中只能用作目的地址。这个特殊的地址使用相应减少了 A 类、B 类和 C 类地址中每一个网络中的可用主机数。

例如,路由器发送数据包,其目的地址为 221.45.71.255,而该网络内采用默认的子网掩码 255.255.255.0 分配 IP 地址,则该网络上以 221.45.71 开头的所有设备都接收和处理这个数据包。

(3) 受限广播地址

在 A,B,C 类地址中,若网络位和主机位都是全 1(32 位),即 255.255.255.255,则该地址用于定义在当前网络上的广播地址。一个主机若想把报文发送给所有其他主机,就可使用这样的地址作为数据包中的目的地址。但路由器把具有这种类型地址的数据包阻挡住,使这样的广播只局限在本地网络。应注意,这种地址属于 E 类。

例如,主机可以发送使用全 1 目的 IP 地址的数据包,在该网络上的所有设备都能接收和处理这个数据包。

(4) 回环地址

第一个字节等于 127 的 IP 地址用作环回地址,该地址用来测试机器的 TCP/IP 协议是否安装正常。当使用这个地址时,数据包默认将本机地址作为目的地址。因此,该地址可用于测试 IP 软件。例如,像"Ping"这样的应用,可以发送把环回地址作为目的地址的数据包,以便测试 IP 软件能否接收和处理数据包。另一个示例是客户进程(运行着的程序)用环回地址发送数据包给相同机器上的服务器进程。应该注意,这种地址在数据包中只能用作目的地址。

6. 专用地址

在每一类地址中都有一些段被指派作为专用地址。这些地址或者用在隔离的情况下,或者用在网络地址转换技术中,见表 1-9。

表 1-9　专用地址分配表

类	网　络　位	网络总数
A	10.0.0	1
B	172.16～172.31	16
C	192.168.0～192.168.255	256

7. 单播、多播和广播地址

Internet 上的通信可用单播、多播和广播地址来完成。

(1) 单播地址

单播通信是一对一的，是从单个源端将数据包发送到单个的目的端。在 Internet 上的所有系统必须至少有一个唯一的单播地址。单播地址可以是 A 类、B 类或 C 类的。

(2) 多播地址

多播又称组播。多播通信是一对多的，是从单个源端把数据包发送到一组目的端。多播地址是 D 类的。它定义了一个组号。在 Internet 上的系统可以有一个或多个 D 类多播地址(除了它的一个或多个单播地址外)。如果某个系统(通常是主机)有 7 个多播地址，表示它属于 7 个不同的组。应该注意，D 类地址只能用作目的地址，不能用作源地址。

Internet 上的多播可以是本地级的，也可以是全局级的。在本地级，局域网上的一些主机可构成一个组，并被指派一个多播地址。在全局级，不同网络上的一些主机可构成一个组，并被指派一个多播地址。

(3) 广播地址

广播通信是一对所有的。Internet 只允许进行本地级广播。在本地级使用两个广播地址，即受限广播地址(全 1)和直接广播地址(主机位全 1)。

广播不允许在全局级进行，这表示一个系统(主机或路由器)不能向 Internet 上的所有主机或路由器发送数据包。

1.3.2 子网划分

IP 地址被设计成两级层次结构，即网络地址和主机地址。然而在很多情况下，这两级层次结构不够用。例如，有一个机构的网络地址是 141.14.0.0(B 类地址)。这个机构有两级层次结构的编址，如图 1-5 所示，该机构拥有的物理网络数却不能大于 1。应当注意，默认子网掩码(255.255.0.0)表示所有地址都有 16 位是相同的，剩下的位定义网络上的不同地址。还应当注意，网络地址是这个地址段的第一个地址；在网络地址中，主机部分是全 0。

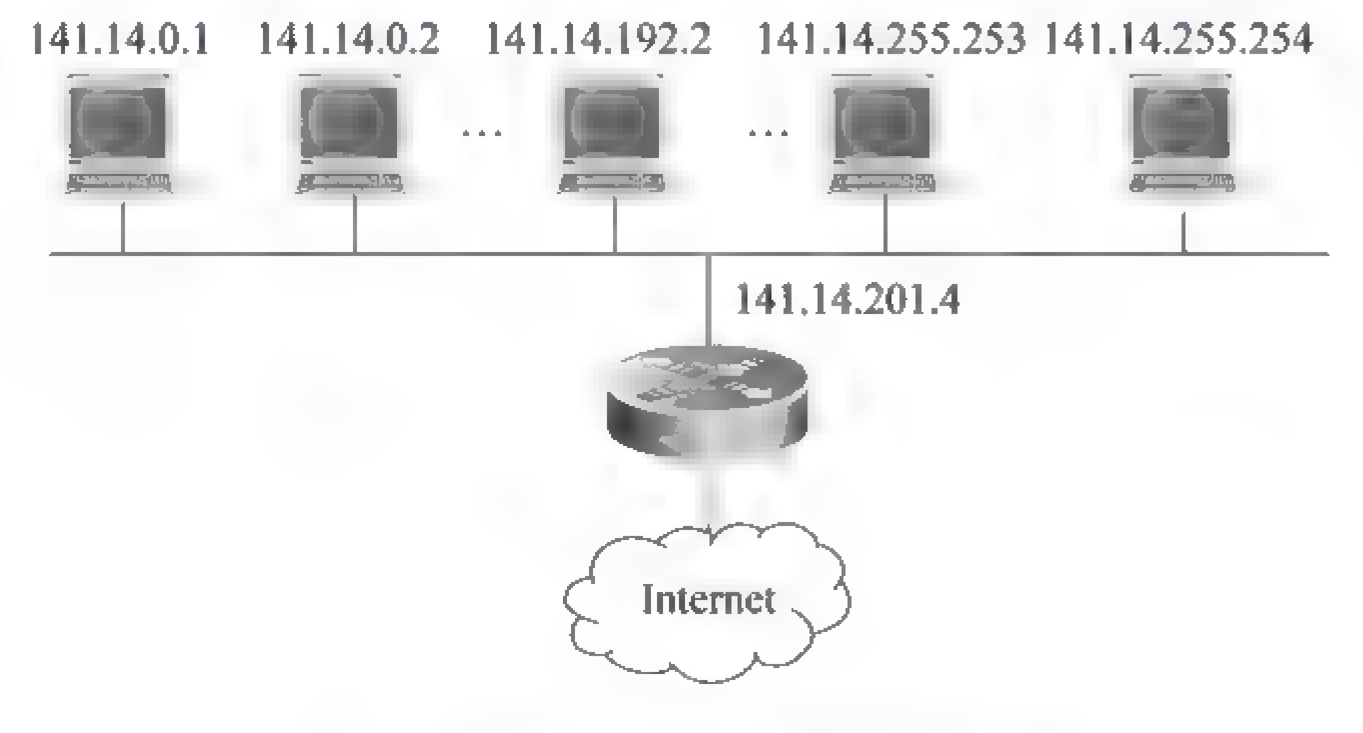


图 1-5 网络地址的两级层次结构

按照上述方案，受到两级层次结构的限制，众多的主机不能再划分为组，所有的主机都在同一个层次上，则该机构只有一个拥有很多主机的网络。

对这个问题的一种解决方法是划分子网，即把一个网络划分为一些更小的网络，称为子网。例如，把图1-5所示的网络再划分为3个子网，如图1-6所示。

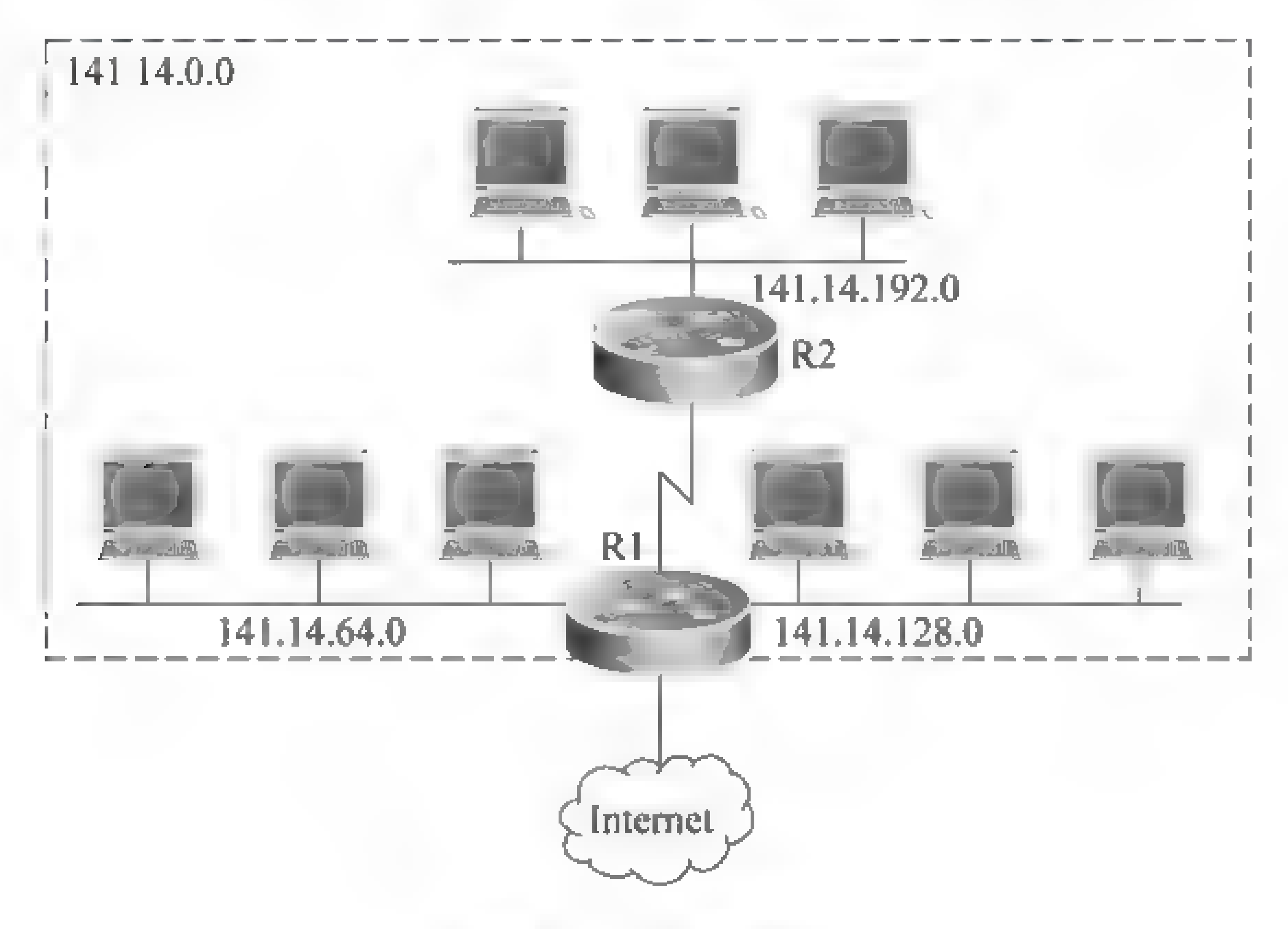


图1-6　子网划分

在以上示例中，Internet的其余部分不知道该网络已划分为三个物理子网，这三个子网对Internet的其余部分来说仍然是一个网络。发送给主机141.14.192.2的数据仍到达路由器R1。当数据到达R1后，对IP地址的解释却改变了。路由器R1知道网络141.14.0.0在物理上已成为三个子网，它知道数据必须交付给子网141.14.192.0。

1. 三级层次结构

增加子网就是在IP地址系统中产生一个中间级的层次。本例中有三级，即主网、子网和主机。主网是第一级，子网是第二级，主机是第三级。那么，IP数据包寻址要经过主网、子网，最后到达主机。这好像公司的电话号码，分为地区号、总机号和分机号三级，如0533-2886688-6001。

2. 子网掩码

当网络没有划分子网时，网络掩码就已经被使用了。网络掩码用于找出地址段的第一个地址，也就是网络地址。当划分子网时，情况就不同了，子网掩码有更多的1。网络掩码产生了网络地址，子网掩码则产生子网地址。

(1) 子网掩码规则

在使用掩码的初期，采用的是不连续子网掩码。所谓不连续子网掩码，是指这些位并非一串1后面跟随一串0，而是将1和0混杂在一起。现在都使用连续的掩码(即一串1后面跟随一串0)。

例如，11111111 11111111 11110000 00000000(即255.255.240.0)是合法的子网掩码，而11111111 11111111 11000011 00000000(即255.255.195.0)是非法的子网掩码。

(2) 计算子网地址

只要给出了 IP 地址，就可以对地址进行掩码运算，找出子网地址。有直接的和快捷的两种方法。

① 直接的方法

使用直接的方法时，把用二进制数表示的地址和掩码进行"与"操作，找出子网地址。

若主机地址是 144.45.34.56，子网掩码是 255.255.240.0，求子网地址的过程如下(对主机地址和子网掩码进行与运算操作)：

```
主机地址   10001000 00101101 00100010 00111000
子网掩码   11111111 11111111 11110000 00000000
子网地址   10001000 00101101 00100000 00000000
```

则子网地址是 144.45.32.0。

② 快捷的方法

若子网掩码是连续的，可以使用快捷的方法，这时要遵循三条规则：

- 若掩码中的字节是 255，复制这个字节到地址中。
- 若掩码中的字节是 0，在地址中用 0 代替这个字节。
- 若掩码中的字节既不是 255 也不是 0，采用二进制写出掩码和地址，然后进行运算。

对于上述示例，采取快捷的方法计算如下：

```
主机地址   144. 45.00100010.56
子网掩码   144.255.11110000. 0
子网地址   144. 45.00100000. 0
```

则子网地址是 144.45.32.0。

(3) 子网数和每一个子网内的地址数

计算在使用子网掩码时给默认掩码增加的 1 的个数，就可以找出子网数。在上例中，额外的 1 的个数为 4，因此子网数是 $2^3=8$。

计算子网掩码中 0 的个数，可找出每一个子网的地址数。在上例中，0 的个数是 12，因此在每一个子网中可能的地址数是 $2^{12}=4096$。

每一个子网中的第一个地址(即主机位全 0)是子网地址，最后一个地址(即主机位全 1)保留在子网内用作受限广播地址。因此，在每一个子网内的有效主机地址数是 2^n-2。

规律总结(检查)

网络是信息基础设施，在社会生活中，信息传递、营销、服务、交流、娱乐等各种活动都可以通过网络完成，网络的质量直接决定了社会生活和经济生活的质量。在计算机网络的质量体系中，网络管理是一个关键环节。网络管理的质量直接影响网络的运行质量。

对于网络管理，管理员除了具备有关基本的连接设备和协议的知识之外，需要重点掌握交换和路由技术，本教材将侧重于介绍这两方面的知识。

在计算机网络系统中，交换概念的提出是对共享工作模式的改进。HUB集线器就是一种共享设备，但HUB本身不能识别目的地址，当同一局域网内的A主机给B主机传输数据时，数据包在以HUB为架构的网络上是以广播方式传输的，由每一台终端通过验证数据包头的地址信息来确定是否接收。也就是说，在这种工作方式下，同一时刻网络上只能有一组数据帧的通信，如果发生碰撞，还得重试。这种方式就是共享网络带宽。

路由器是互联网的主要节点设备。路由器通过路由决定数据的转发。转发策略称为路由选择(routing)，这也是路由器名称的由来(router，转发者)。作为不同网络之间互相连接的枢纽，路由器系统构成了基于TCP/IP的国际互联网Internet的主体脉络，也可以说，路由器构成了Internet的骨架。它的处理速度是网络通信的主要瓶颈之一，其可靠性直接影响着网络互联的质量。因此，在园区网、地区网，乃至整个Internet研究领域中，路由器技术始终处于核心地位，其发展历程和方向成为整个Internet研究的一个缩影。

网络管理不是新概念。从广义上讲，任何一个系统都需要管理，只是由于系统的大小和复杂性的不同，管理在整个系统中的重要性有所不同。网络也是一个系统。虽然网络管理很早就有，却一直没有得到应有的重视。这是因为以前的网络规模较小，而且复杂性不高，一个简单的网络管理系统就可以满足网络正常运行的需要，因而对其研究较少。但随着网络规模逐渐增大，复杂性增加，网络管理技术凸显其重要性，而且网络要正常运行，对于网络管理的依赖性越来越大。

拓展提高(拓展)

1. 网络设备的IOS恢复问题

由于在路由器或交换机的配置过程中操作失误，致使路由器IOS操作系统丢失，导致设备无法进入正常工作状态，这时候该怎么恢复呢？

首先，在一台PC机上安装TFTP服务器软件，将IOS文件放置在TFTP服务器的默认根目录下，打开TFTP服务器，用控制线将这台机器与路由器连接起来，用交叉网线连接机器的网卡和路由器的以太口(也可以用普通的网线将路由器和交换机相连，再连接机器)。

然后，打开机器的超级终端工具，连接路由器，此时窗口中出现的命令行提示符为：

```
ROMMON 1> (其中"1"代表命令行的行数)
```

在提示符后输入命令。ROMMON＞是操作系统丢失的情况下，网络设备的配置模式。具体操作步骤如下：

```
ROMMON 1> IP_ADDRESS=路由器的 IP 地址 (要和 TFTP 服务器在同一网段内)
ROMMON 2> IP_SUBNET_MASK=路由器的子网掩码
ROMMON 3> DEFAUT_GATEWAY=默认网关地址 (可以没有，也可以是 TFTP 服务器)
ROMMON 4> TFTP_SERVER=TFTP 服务器 IP 地址
ROMMON 5> TFTP_FILE=IOS 文件名 (只给出文件名，不需要路径)
```

```
ROMMON 6>tftpdnld (按 Enter 键)
```

注意：前面的几条命令必须使用大写，最后的 tftpdnld 要用小写。

在 tftpdnld 命令执行后，只要根据提示选择，就可完成文件的传输。当文件传输完成后，将自动回到命令行下，输入“reset”重启路由器，将回到 IOS 模式。此时，甚至连以前配置的信息都将恢复。

2. 设计子网实例

为了更好地理解子网划分，下面给出网络管理员设计公司子网的实例。操作步骤如下。

(1) 决定子网数

决定子网数就是确定公司需要的子网数。作出决定所根据的几个因素是公司的物理位置(建筑物和楼层的数目)、部门数、每一个子网需要的主机数，等等。子网数必须为 2 的若干次方(0,2,4,8,16,32,…)。应当注意，选择 0 表示不划分子网。

(2) 找出子网掩码

找出子网掩码就是要找出连续的子网掩码。下面的规则可帮助网络管理员很容易地找出子网掩码：

① 找出默认掩码中的 1 的个数。

② 找出定义子网的 1 的个数。

③ 把规则①和②中的 1 的个数相加。

④ 找出 0 的个数，它等于 32 减去规则③得出的 1 的个数。

(3) 找出每一个子网的地址范围

在确定子网掩码之后，网络管理员就能找出每一个子网的地址范围。有两种方法用来寻找每一个子网的第一个和第二个地址。

第一种方法是从第一个子网开始。第一个子网的第一个地址是该地址段的第一个地址，加上每一个子网的地址数可得出最后一个地址。然后，把该地址加 1，找出下一个子网的第一个地址。对这个子网重复以上过程。

第二种方法是从最后一个子网开始。最后一个子网的最后一个地址是该地址段的最后一个地址，通过掩码运算可获得子网的第一个地址。然后，把该地址减 1，找出倒数第二个子网的最后一个地址。对这个子网重复以上过程。

例如，某个公司分到的地址是 201.70.64.0(C 类)。该公司需要 6 个子网，试设计子网。解决这个问题的分析过程如下：

① 默认掩码的个数是 24(C 类)。

② 公司需要 6 个子网，但 6 不是 2 的整数次方，其下一个 2 的整数次方是 8(2 的 3 次方)，则子网掩码中需要有 3 个 1。

③ 子网掩码中 1 的个数是 27(24+3)。

④ 子网掩码中 0 的个数是 5(32－27)。

⑤ 子网掩码的二进制表示是 11111111 11111111 11111111 11100000，点分十进制表示是 255.255.255.224。

⑥ 子网数是 8。

⑦ 每个子网中的地址数是 25(5 是 0 的个数)或 32。

⑧ 采用第一种方法找出地址范围。从第一个子网开始，其第一个地址是 201.70.64.0(地址段中的第一个地址)；最后一个地址是在第一个地址上加 31(每一个子网的地址数是 32，但只能加 31)，得到 201.70.64.31。

⑨ 找出第二个子网的地址范围，其第一个地址是 201.70.64.32(在第一个子网的最后一个地址的后面)；最后一个地址是在第一个地址上加 31，得出 201.70.64.63。

⑩ 在剩下的子网中，地址是范围采用类似的方法求出。

思考训练(评估)

1. 思考与提高

(1) 网络设备操作系统的作用是什么？

(2) 连接网络设备有哪几种方式？

(3) 简述 IP 地址的作用及其分类方法。

(4) 简述子网划分的方法。

2. 实训

(1) 练习使用 telnet 登录交换机。

(2) 若主机地址是 19.30.80.5，网络掩码是 255.255.192.0，试求子网地址和广播地址。

(3) 某个公司分到的地址是 201.70.64.0(C 类)。该公司需要 6 个子网，试设计子网。

学习情境 2 局域网中的广播流量管理

任务情境(资讯)

张三和李四在大学是室友,他们平时为导师编写程序。毕业后,两人自主创业,成立了一个小型软件公司,主要业务是软件开发。经过几年的发展,公司慢慢壮大起来。2008 年,张三和李四开发的一套软件在市场上取得了巨大的成功。在风险投资的资金支持下,他们又成立了 ThreeFour Software 软件公司,有 40 名员工,租用了 400 多平方米的办公室。这时就需要将公司里的服务器和 PC 机用网络设备连接起来。考察当前市场的主流产品后,他们选用两台 24 口 Cisco 交换机来作为网络连接设备。

随着公司网络规模的增大,在运行的过程中,有员工抱怨网络速度越来越慢,交换机也时常处于满负荷工作状态。李四在交换机的端口上观察流量,发现在网络中有大量的广播报文出现,这严重地影响了交换机的性能。

为了解决广播风暴的问题,李四在整个网络中划分了 VLAN,两个从事软件开发的工作组分属两个 VLAN,张三、李四以及其他市场人员属于一个 VLAN。这样做隔离了广播域,有效地抑制了广播风暴。由于公司所有的 PC 都连接在两台交换机上,所以在两台交换机上都配置了三个相应的 VLAN,交换机之间的端口也都配置成 Trunk 端口并允许三个 VLAN 通过。VLAN 建好后,李四发现不同 VLAN 的主机之间无法互相访问。这时,需要一个三层设备来进行 VLAN 之间的转发。

在增加了一台三层交换机之后,公司网络中的跨 VLAN 通信问题得到了解决。但是又出现了新的问题:跨 VLAN 的数据流量都先送到三层交换机,而且在同一 VLAN 但分属不同二层交换机的流量也会通过三层交换机。这样,若任意一条连接二层交换机和三层交换机的链路断开,都会对网络中的数据传输造成较大的影响。

为此,需要提高网络的可靠性,增加一条连接两台二层交换机的冗余链路,即使任意一条链路断开,网络仍然可以保持连通。但新增一条冗余链路之后,部分主机将无法访问,交换机流量明显增大,特别是广播流量增加,交换机又处于满负荷工作状态。

任务分析(决策)

在上述情境中有两个核心问题,即 VLAN 的划分和网络中冗余链路的产生及相应的解决办法。为了解决这两个问题,需要掌握以下理论。

1. VLAN 的内含

VLAN(Virtual Local Area Network)即虚拟局域网。LAN 可以是由几台家用计算

机构成的网络，也可以是由数以百计的计算机构成的企业网络。VLAN 所指的 LAN 特指使用路由器分割的网络，也就是广播域。

广播域指的是广播帧（目标 MAC 地址全部为 1）所能传递到的范围，即能够直接通信的范围。严格地说，不仅仅是广播帧，多播帧（Multicast Frame）和目标不明的单播帧（Unknown Unicast Frame）也能在同一个广播域中畅行无阻。

本来，二层交换机只能构建单一的广播域，但在使用 VLAN 功能后，它能够将网络分割成多个广播域。那么，为什么需要分割广播域呢？因为如果仅有一个广播域，可能影响到网络整体的传输性能。

图 2-1 所示是一个由 5 台二层交换机（交换机 1～5）连接大量客户机构成的网络。假设计算机 A 需要与计算机 B 通信，在基于以太网的通信中，必须在数据帧中指定目标 MAC 地址才能正常通信，因此计算机 A 必须先广播“ARP 请求（ARP Request）信息”来尝试获取计算机 B 的 MAC 地址。

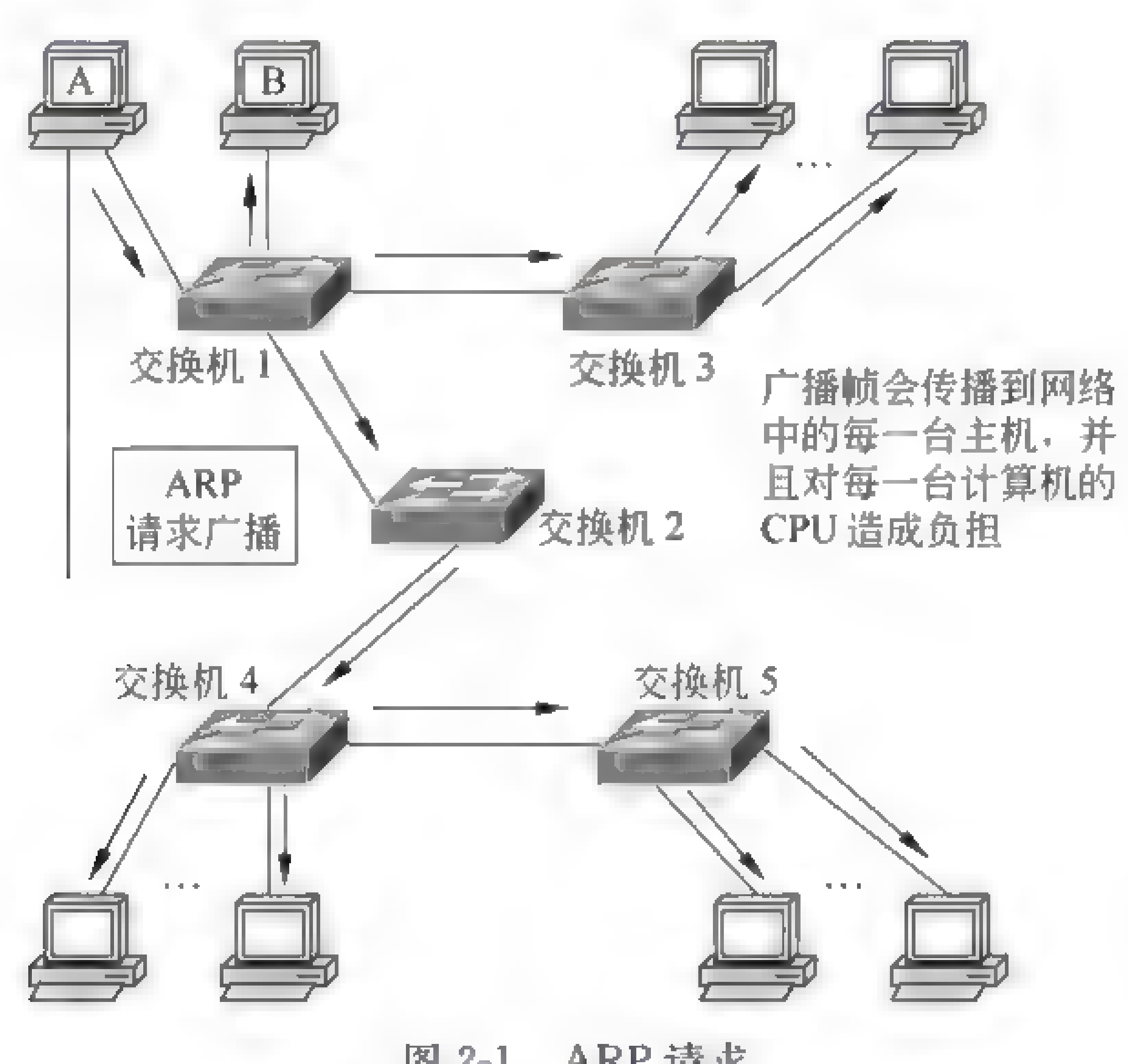


图 2-1　ARP 请求

交换机 1 收到广播帧（ARP 请求）后，将它转发给除接收端口外的其他所有端口，也就是 Flooding（泛洪）了。交换机 2 收到广播帧后也会 Flooding。交换机 3、4、5 也会 Flooding。最终，ARP 请求被转发到同一个网络中的所有客户机上。

这个 ARP 请求原本是为了获得计算机 B 的 MAC 地址而发出的。也就是说，只要计算机 B 能收到就可以了。但是事实上，数据帧传遍整个网络，导致所有的计算机都收到了它。如此一来，一方面，广播信息消耗了网络带宽；另一方面，收到广播信息的计算机还要消耗一部分 CPU 时间来对它进行处理，造成网络带宽和 CPU 运算能力的大量无谓消耗。

也许人们会有这样的问题：广播信息是这样经常发出的吗？广播信息真是那么频繁出现吗？是的，实际上，广播帧会非常频繁地出现。利用 TCP/IP 协议栈通信时，除了前面出现的 ARP 外，还有可能需要发出 DHCP（Dynamic Host Configuration Protocol，动态主机分配协议）、RIP（Routing Information Protocol，路由信息协议）等很多其他类型的

广播信息。

ARP 广播是在需要与其他主机通信时发出的。当客户机请求 DHCP 服务器分配 IP 地址时，必须发出 DHCP 广播。使用 RIP 作为路由协议时，每隔 30s，路由器会对邻近的其他路由器广播一次路由信息。RIP 以外的其他路由协议使用多播传输路由信息，也会被交换机转发(Flooding)。除了 TCP/IP 以外，NetBEUI、IPX 和 AppleTalk 等协议也经常需要用到广播。例如，在 Windows 下双击打开“网络计算机”时会发出广播(多播)信息(Windows XP 除外)。

总之，广播就在我们身边。下面列出的是一些常见的广播通信：

① ARP 请求：建立 IP 地址和 MAC 地址的映射关系。

② RIP：一种路由协议。

③ DHCP：用于自动设定 IP 地址的协议。

④ NetBEUI：Windows 下使用的网络协议。

⑤ PX：Novell Netware 使用的网络协议。

⑥ AppleTalk：苹果公司的 Macintosh 计算机使用的网络协议。

如果整个网络只有一个广播域，那么一旦发出广播信息，就会传遍整个网络，并且对网络中的主机带来额外的负担。因此，在设计 LAN 时，需要注意有效地分割广播域。

2. 采用 VLAN 的目的

VLAN 技术主要解决交换机在进行局域网互联时无法限制广播的问题。它把一个 LAN 划分成多个逻辑上的 LAN ——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，VLAN 间不能直接互通，将广播报文限制在一个 VLAN 内。

3. 冗余链路

在骨干网设备连接中，单一链路的连接很容易实现，但一个简单的故障就会造成网络中断。因此，在实际网络组建的过程中，为了保持网络的稳定性，在由多台交换机组成的网络环境中，通常使用备份连接。以提高网络的健壮性、稳定性。

备份连接也称为备份链路或者冗余链路。备份链路之间的交换机经常互相连接，形成环路，在一定程度上实现冗余。

链路的冗余备份使网络的健壮性、稳定性和可靠性得到提高，但是备份链路使网络存在环路。交换机之间的环路将导致广播风暴、多帧复制和地址表的不稳定等问题。

4. 链路聚合

链路聚合是指将两条或更多条数据信道结合成一条信道，该信道以单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备，例如连接骨干网络的服务器或服务器群。

如果聚合的每条链路都遵循不同的物理路径，则聚合链路也提供冗余和容错。通过聚合调制解调器链路或者数字线路，链路聚合可用于改善对公共网络的访问。链路聚合也可用于企业网络，以便在吉比特以太网交换机之间构建多条吉比特的主干链路。

采用链路聚合后，逻辑链路的带宽增加了大约(n－1)倍，这里，n为聚合的路数。另外，聚合后，链路可靠性大大提高，因为n条链路中只要有一条可以正常工作，则聚合后的这条链路就可以工作。除此之外，链路聚合可以实现负载均衡。因为对于通过链路聚合连接在一起的两台(或多台)交换机(或其他网络设备)，通过内部控制，可以合理地将数据分配在被聚合连接的设备上，实现负载分担。

这里涉及的链路聚合又称端口聚合或端口捆绑，英文名称是Port Trunking，其功能是将交换机的多个低带宽端口捆绑成一条高带宽链路，实现链路负载平衡，避免链路出现拥塞现象。通过配置，可将两个、三个或是四个端口进行捆绑，分别负责特定端口的数据转发，防止单条链路转发速率过低而出现丢包的现象。

Trunking的优点是价格便宜，性能接近千兆以太网；不需要重新布线，也无须考虑千兆网传输距离极限问题；Trunking可以捆绑任何相关的端口，也可以随时取消设置，具有很高的灵活性，提供了负载均衡能力以及系统的容错性。

5. 生成树协议

(1) 技术原理

生成树协议(STP，Spanning Tree Protocol)的基本思想就是生成“一棵树”，树的根是一台称为根桥的交换机，根据设置的不同，不同的交换机会被选为根桥，但任意时刻只能有一个根桥。由根桥开始，逐级形成一棵树，根桥定时发送配置报文，非根桥接收配置报文并转发。如果某台交换机能够从两个以上的端口接收到配置报文，说明从该台交换机到根有不止一条路径，构成了循环回路，此时交换机根据端口的配置选出一个端口并把其他端口阻塞，消除循环。当某个端口长时间不能接收到配置报文的时候，交换机认为端口的配置超时，网络拓扑可能已经改变，此时重新计算网络拓扑，重新生成一棵树。

(2) 功能介绍

生成树协议最主要的应用是为了避免局域网中的网络环回，解决成环以太网的“广播风暴”问题。从某种意义上说，它是一种网络保护技术，可以消除由于失误或者意外带来的循环连接。STP能够为网络提供备份连接，可与SDH(Synchronous Digital Hierarchy，同步数字系列)保护配合构成以太环网的双重保护。新型以太单板支持符合IEEE 802.1d标准的生成树协议STP及802.1w规定的快速生成树协议(RSTP，Rapid Spaning Tree Protocol)，收敛速度可达到1s。

生成树协议的主要功能有两个：一是利用生成树算法，在以太网中创建一个以某台交换机的某个端口为根的生成树，避免环路；二是在以太网拓扑发生变化时，通过生成树协议达到收敛保护的目的。

① 生成树协议避免环路

每个LAN都会选择一台设备为指定交换机，通过该设备的端口连接到根，该端口为指定端口(DP，Designated Port)。

将交换网络中所有设备的根端口(RP)和指定端口(DP)设为转发状态(Forwarding)，将其他端口设为阻塞状态(Blocking)。生成树经过一段时间(默认值是50s)稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。

② 生成树协议对网络的收敛保护

STP 操作对于终端来说是透明的，而不管终端是连在 LAN 的某一个部分还是多个部分。当创建网络时，网络中的所有节点之间存在多条路径。

每个 VLAN 是一个逻辑 LAN 部分，所以网管人员能使 STP 一次工作在最多 64 个 VLAN 中。如果要配置超过 64 个 VLAN，网管人员需要将其他 VLAN 的 STP 禁止，因为默认的 STP 可以支持 1～64 个 VLAN。

任务设计（计划）

在简单了解用于局域网连接的基本方法后，下面根据 ThreeFour Software 公司的具体情况来讨论，主要完成以下 5 个任务：

任务 2.1　实现 VLAN 的机制

任务 2.2　VLAN 的配置与管理

任务 2.3　VLAN 的汇聚链接、VLAN 间路由

任务 2.4　交换网络中的冗余链路管理

任务 2.5　配置生成树协议（STP/RSTP）

任务实施（实施）

任务 2.1　实现 VLAN 的机制

2.1.1　使用 VLAN 分割广播域

在理解了“为什么需要 VLAN”之后，接下来讨论交换机是如何使用 VLAN 分割广播域的。

首先，在一台未设置任何 VLAN 的二层交换机上，任何广播帧都会被转发给除接收端口外的所有其他端口（Flooding）。例如，计算机 A 发送广播信息后，会被转发给端口 2、3 和 4。这时，如果在交换机上生成 VLAN 1 和 VLAN 2，同时设置端口 1 和 2 属于 VLAN 1，端口 3 和 4 属于 VLAN 2，再从 A 发出广播帧的话，交换机只会把它转发给同属于一个 VLAN 的其他端口，也就是同属于 VLAN 1 的端口 2，而不会转发给属于 VLAN 2 的端口。

同样，C 发送广播信息时，只会转发给属于 VLAN 2 的端口 4，而不会转发给属于 VLAN 1 的端口，如图 2-2 所示。

就这样，VLAN 通过限制广播帧转发的范围分割了广播域。图中为了便于说明，以红、蓝两色识别不同的 VLAN，在实际中用“VLAN ID”来区分。这里的 ID 用于标识不同的 VLAN，其范围是 1～4094。

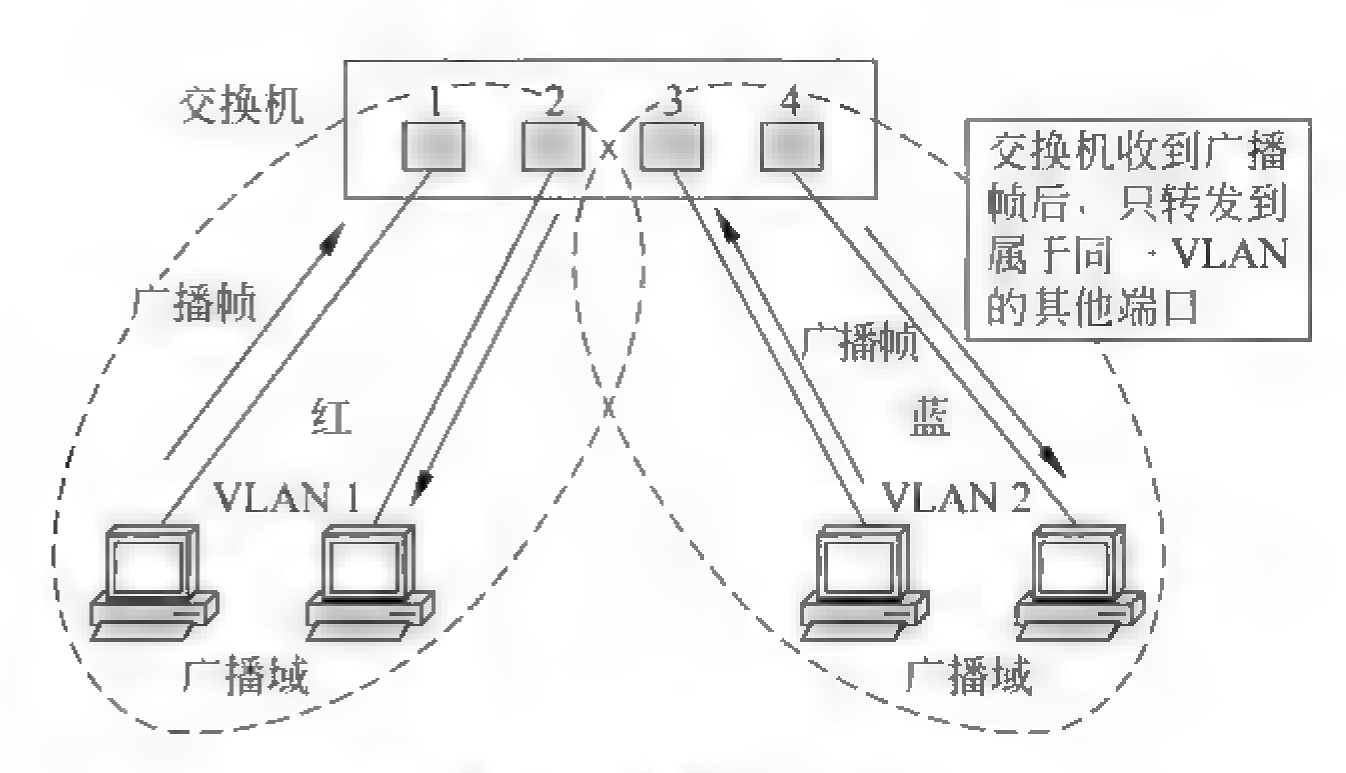


图 2-2　设置 VLAN

2.1.2　直观地描述 VLAN

如果要更直观地描述 VLAN，可以理解为将一台交换机在逻辑上分割成数台交换机。在一台交换机上生成 VLAN 1 和 VLAN 2，相当于将一台交换机看做是两台虚拟的交换机。如图 2-3 所示，在两个 VLAN 之外生成新的 VLAN 时，可以想象成添加了新的交换机。

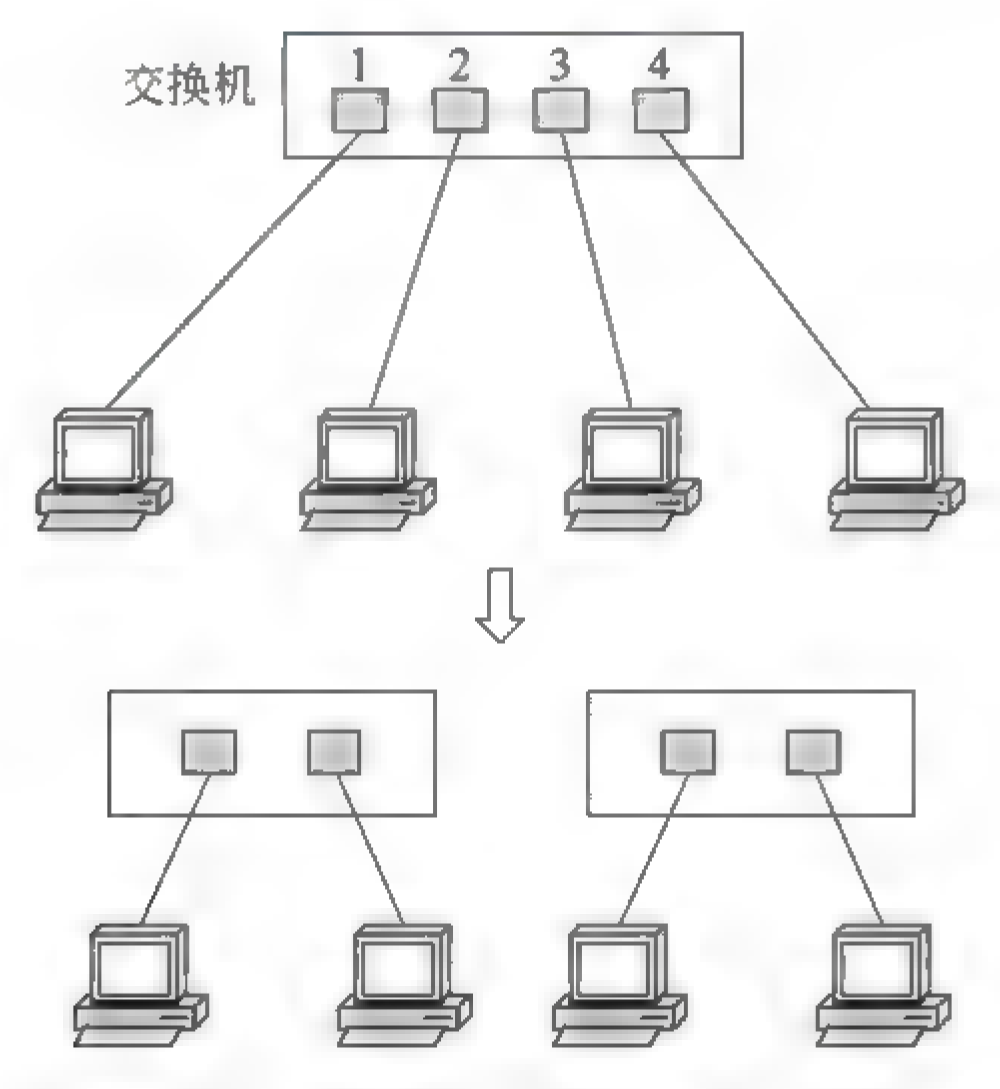


图 2-3　将一台交换机看做两台虚拟的交换机

但是，VLAN 生成的逻辑上的交换机是互不相通的。因此，在交换机上设置 VLAN 后，如果未做其他处理，VLAN 间无法通信。

明明接在同一台交换机上，却偏偏无法通信，这个事实也许让人难以接受。但它既是 VLAN 方便易用的特征，又是 VLAN 令人难以理解的原因。

2.1.3 划分 VLAN

1. 根据端口划分 VLAN

许多 VLAN 厂商都利用交换机的端口来划分 VLAN 成员，被设定的端口都在同一个广播域中。例如，一个交换机的 1，2，3，4，5 端口被定义为虚拟网 AAA，同一台交换机的 6，7，8 端口组成虚拟网 BBB。这样做，允许各端口之间通信，并允许共享型网络的升级。但是，这种划分模式将虚拟网限制在了一台交换机上。

第二代端口 VLAN 技术允许跨越多台交换机的多个不同端口划分 VLAN，不同交换机上的若干个端口可以组成同一个虚拟网。

以交换机端口来划分网络成员，其配置过程简单明了，是最常用的一种方式。

2. 根据 MAC 地址划分 VLAN

这种方法是根据每个主机的 MAC 地址来划分，即对每个 MAC 地址的主机都配置它属于哪个组。这种方法的最大优点是当用户物理位置移动，即从一台交换机换到其他交换机时，VLAN 不用重新配置，所以这种划分方法基于用户的 VLAN。其缺点是初始化时，所有用户都必须配置，如果用户较多，配置工作将非常繁重；而且这种方法导致交换机执行效率降低，因为在每一台交换机端口都可能存在很多个 VLAN 组的成员，无法限制广播包。另外，对于使用笔记本电脑的用户来说，他们的网卡可能经常更换，必须经常配置 VLAN。

3. 根据网络层划分 VLAN

这种方法是根据每个主机的网络层地址或协议类型（如果支持多协议）划分的。虽然这种划分方法是根据网络地址，比如 IP 地址，但它不是路由，与网络层的路由毫无关系。

这种方法的优点是当用户的物理位置改变时，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，这对网络管理者来说很重要。还有，这种方法不需要附加的帧标签来识别 VLAN，减少了网络通信量。

这种方法的缺点是效率低，因为检查每一个数据包的网络层地址需要处理时间（相对于前面两种方法），一般的交换机芯片都可以自动检查网络上数据包的以太网帧头，但要让芯片检查 IP 帧头，需要更高的技术，也更费时。当然，这与各个厂商的实现方法有关。

4. 根据 IP 组播划分 VLAN

IP 组播实际上也是一种 VLAN 的定义，即认为一个组播组就是一个 VLAN。这种划分方法将 VLAN 扩大到广域网，因此具有更大的灵活性，也很容易通过路由器进行扩展。这种方法不适合局域网，主要原因是效率不高。

5. 基于规则的 VLAN

基于规则的 VLAN 也称为基于策略的 VLAN。这是最灵活的 VLAN 划分方法，具有自动配置的能力，能够把相关的用户连成一体，在逻辑划分上称为“关系网络”。网络管理员只需在网管软件中确定划分 VLAN 的规则(或属性)，当一个站点加入网络时，将会被“感知”，并被自动地包含进正确的 VLAN。同时，对站点的移动和改变也可自动识别和跟踪。

采用这种方法，整个网络可以非常方便地通过路由器扩展网络规模。有的产品还支持一个端口上的主机分别属于不同的 VLAN，这在交换机与共享式 HUB 共存的环境中显得尤为重要。自动配置 VLAN 时，交换机软件自动检查进入交换机端口的广播信息的 IP 源地址，然后将端口分配给一个由 IP 子网映射成的 VLAN。

6. 按用户定义、非用户授权划分 VLAN

基于用户定义、非用户授权来划分 VLAN，是指为了适应特别的 VLAN 网络，根据网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问 VLAN，但是需要提供用户密码，在得到 VLAN 管理认证后才可以加入一个 VLAN。

对于以上介绍的划分 VLAN 的方式，基于端口的 VLAN 端口方式建立在物理层上；MAC 方式建立在数据链路层上；网络层和 IP 广播方式建立在第三层上。

2.1.4 VLAN 的标准

本节只介绍两种比较通用的 VLAN 标准，一些公司有自己的标准，比如 Cisco 公司的 ISL 标准，虽然不是通用标准，但是由于 Cisco Catalyst 交换机的大量使用，它成为一种“不是标准的标准”。

1. 802.10 VLAN 标准

1995 年，Cisco 公司提倡使用 IEEE 802.10 协议。在此之前，IEEE 802.10 曾经在全球范围内作为 VLAN 安全性的统一规范。Cisco 公司试图采用优化后的 802.10 帧格式在网络上传输 Frame Tagging 模式中所必需的 VLAN 标签。然而，大多数 802 委员会成员都反对推广 802.10，因为该协议是基于 Frame Tagging 方式的。

2. 802.1q

1996 年 3 月，IEEE 802.1 Internet Working 委员会结束了对 VLAN 初期标准的修订工作。新出台的标准进一步完善了 VLAN 的体系结构，统一了 Frame Tagging 方式中不同厂商的标签格式，并制定了 VLAN 标准在未来一段时间内的发展方向，形成的 802.1q 标准在业界获得了推广，成为 VLAN 史上的里程碑。802.1q 的出现打破了虚拟网依赖于单一厂商的僵局，从一个侧面推动了 VLAN 的迅速发展。另外，来自市场的压力使各大网络厂商立刻将新标准融合到各自的产品中。

3. Cisco ISL 标准

ISL(Inter Switch Link)是 Cisco 公司的专有封装方式，只能在 Cisco 的设备上支持。ISL 是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，直接在交换机的端口配置 ISL 封装，可跨越交换机进行整个网络的 VLAN 分配和配置。

2.1.5 VLAN 的简单配置

(1) 创建 VLAN 10

```
Switch(config)#VLAN 10
```

(2) 删除 VLAN 10

```
Switch(config)#no VLAN 10
```

(3) 查看 VLAN 的配置

```
Switch#show VLAN brief
```

(4) 在 VLAN 10 中添加端口 f0/2

```
Switch(config)#interface f0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport VLAN 10
```

(5) 在 VLAN 10 中删除 f0/2

```
Switch(config)#interface f0/2
Switch(config-if)#no switchport VLAN 10
```

任务 2.2 VLAN 的配置与管理

情境回顾：随着公司网络规模的增大，在运行的过程中，有员工抱怨网络速度越来越慢，交换机时常处于满负荷工作状态。李四在交换机的端口上观察流量，发现在网络中有大量的广播报文出现，这严重地影响了交换机的性能。

为了解决广播风暴的问题，李四在整个网络中划分了 VLAN，两个从事软件开发的工作组分属两个 VLAN，张三、李四以及其他市场人员属于一个 VLAN。这样做隔离了广播域，有效地抑制了广播风暴。

那么通过什么方法实现端口间的隔离呢？这里划分了 3 个 VLAN，分别定义为 VLAN 10、VLAN 20 和 VLAN 30，其拓扑环境如图 2-4 所示，包括 Cisco 1900 交换机 1 台和 PC 3 台。

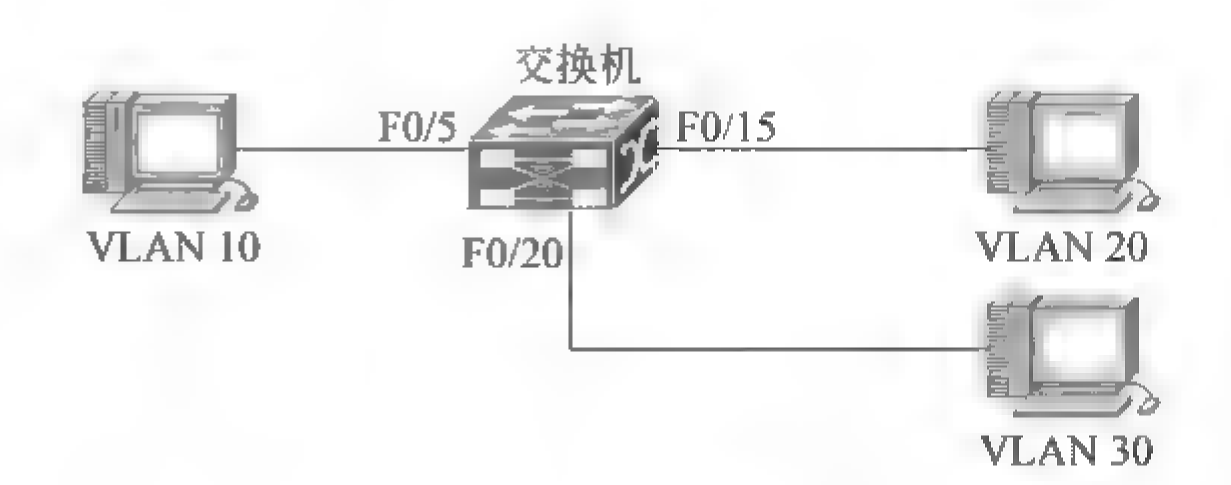


图 2-4　网络拓扑

(1) 在未划分 VLAN 前,两台 PC 可以 ping 通

(2) 创建 VLAN

```
switch #configure terminal                  !进入交换机全局配置模式
switch (config)#vlan 10                     !创建 vlan 10
switch (config-vlan)#name test10            !将 vlan 10 命名为 test10
switch (config)#vlan 20                     !创建 vlan 20
switch (config-vlan)#name test20            !将 vlan 20 命名为 test20
switch (config)#vlan 30                     !创建 vlan 20
switch (config-vlan)#name test30            !将 vlan 30 命名为 test30
switch (config-vlan)#end
switch #show vlan                           !查看 VLAN 划分情况

VLAN Name             Status           Ports
---------------------------------------------------------
1    default          active      Fa0/1, Fa0/2, Fa0/3
                                  Fa0/4, Fa0/5, Fa0/6
                                  Fa0/7, Fa0/8, Fa0/9
                                  Fa0/10, Fa0/11, Fa0/12
                                  Fa0/13, Fa0/14, Fa0/15
                                  Fa0/16, Fa0/17, Fa0/18
                                  Fa0/19, Fa0/20, Fa0/21
                                  Fa0/22, Fa0/23, Fa0/24
10   test10           active
20   test20           active
30   test30           active
```

(3) 将接口分配到 VLAN

```
switch (config)#interface fastEthernet 0/5        !进入 fastethernet 0/5 的接口配置模式
switch (config-if)#switchport access vlan 10      !将 fastethernet 0/5 端口加入 vlan 10
switch (config-if)#exit
switch (config)#interface fastEthernet 0/15       !进入 fastethernet 0/15 的接口配置模式
switch (config-if)#switchport access vlan 20      !将 fastethernet 0/15 端口加入 vlan 20
switch (config-if)#exit
switch (config)#interface fastEthernet 0/20       !进入 fastethernet 0/20 的接口配置模式
switch (config-if)#switchport access vlan 30      !将 fastethernet 0/20 端口加入 vlan 30
switch (config-if)#end
switch #show vlan                                 !查看 VLAN 的端口划分情况
```

```
VLAN Name              Status              Ports
-------------------------------------------------------------------
1    default           active         Fa0/1 ,Fa0/2 ,Fa0/3
                                      Fa0/4 ,Fa0/6 ,Fa0/7
                                      Fa0/8 ,Fa0/9 ,Fa0/10
                                      Fa0/11,Fa0/12,Fa0/13
                                      Fa0/14,Fa0/16,Fa0/17
                                      Fa0/18,Fa0/19,Fa0/21
                                      Fa0/22,Fa0/23,Fa0/24
10   test10            active         Fa0/5
20   test20            active         Fa0/15
30   test30            active         Fa0/20
```

(4) 两台 PC 互相 ping 不通

(5) 将一组接口分配到 VLAN

```
switch #configure terminal
switch (config)#interface range fastEthernet 0/1 -10        !进入接口组配置模式
switch (config-if-range)#switch access vlan 10              !将接口组加入 vlan 10
switch (config-if-range)#end
switch #show vlan
```

```
VLAN Name              Status              Ports
-------------------------------------------------------------------
1    default           active           Fa0/11,Fa0/12,Fa0/13
                                        Fa0/14,Fa0/16,Fa0/17
                                        Fa0/18,Fa0/19, Fa0/21
                                        Fa0/22,Fa0/23, Fa0/24
10   test10            active           Fa0/1,Fa0/2,Fa0/3
                                        Fa0/4,Fa0/5,Fa0/6
                                        Fa0/7,Fa0/8,Fa0/9
                                        Fa0/10
20   test20            active           Fa0/15
30   test30            active           Fa0/20
```

任务 2.3 VLAN 的汇聚链接、VLAN 间路由

情境回顾：VLAN 建好后，李四发现不同 VLAN 的主机之间无法互相访问。这时，需要一台三层设备来进行 VLAN 之间的转发。

2.3.1 VLAN 的汇聚链接(相同 VLAN 通信)

1. 需要设置跨越多台交换机的 VLAN 时，交换机将如何连接呢？

到此为止，我们学习的都是使用单台交换机设置 VLAN 时的情况。那么，如果需要

设置跨越多台交换机的 VLAN，又如何呢？

在规划企业级网络时，可能会遇到隶属于同一部门的用户分散在同一座建筑物中的不同楼层的情况，这时需要考虑跨越多台交换机设置 VLAN 的问题。假设有如图 2-5 所示的网络，且需要将不同楼层的计算机 A、C 和计算机 B、D 设置在同一个 VLAN。

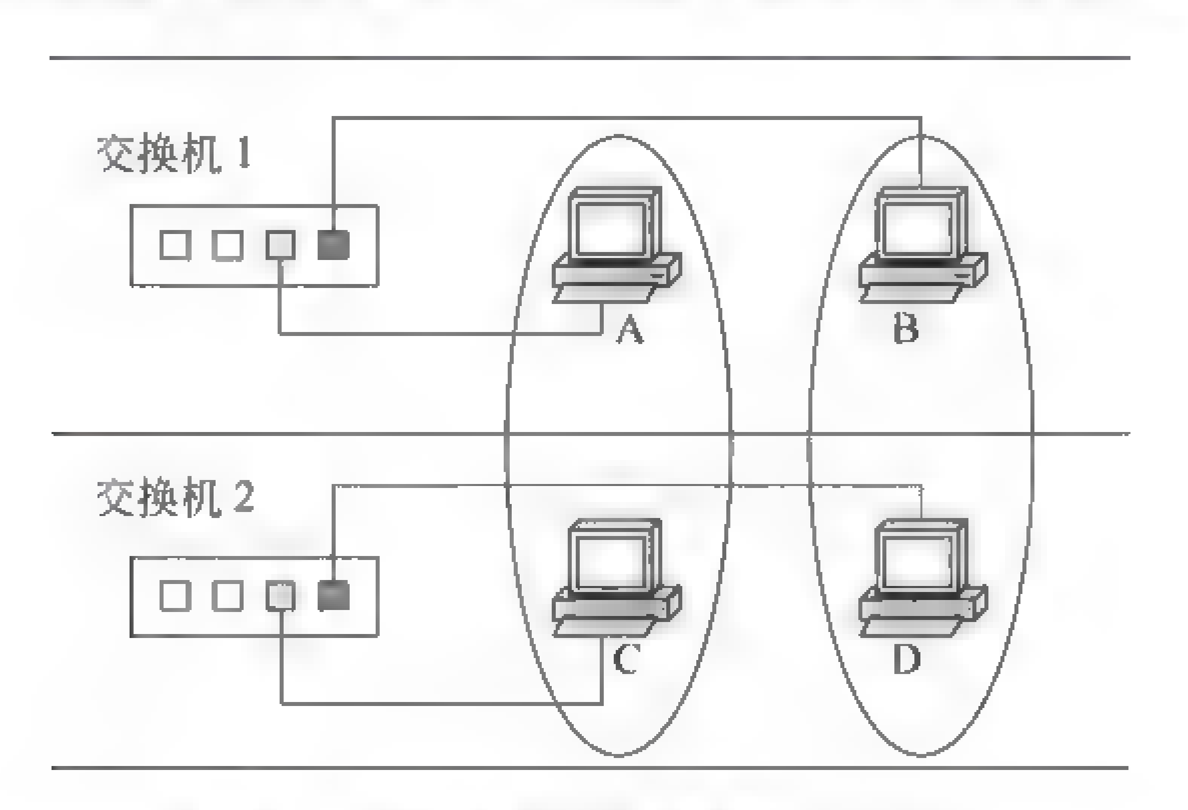


图 2-5 跨越多台交换机的 VLAN

这时最关键问题的就是"交换机 1 和交换机 2 的连接"，最简单的方法是在交换机 1 和交换机 2 上各设一个 VLAN 专用的接口并互联，如图 2-6 所示。

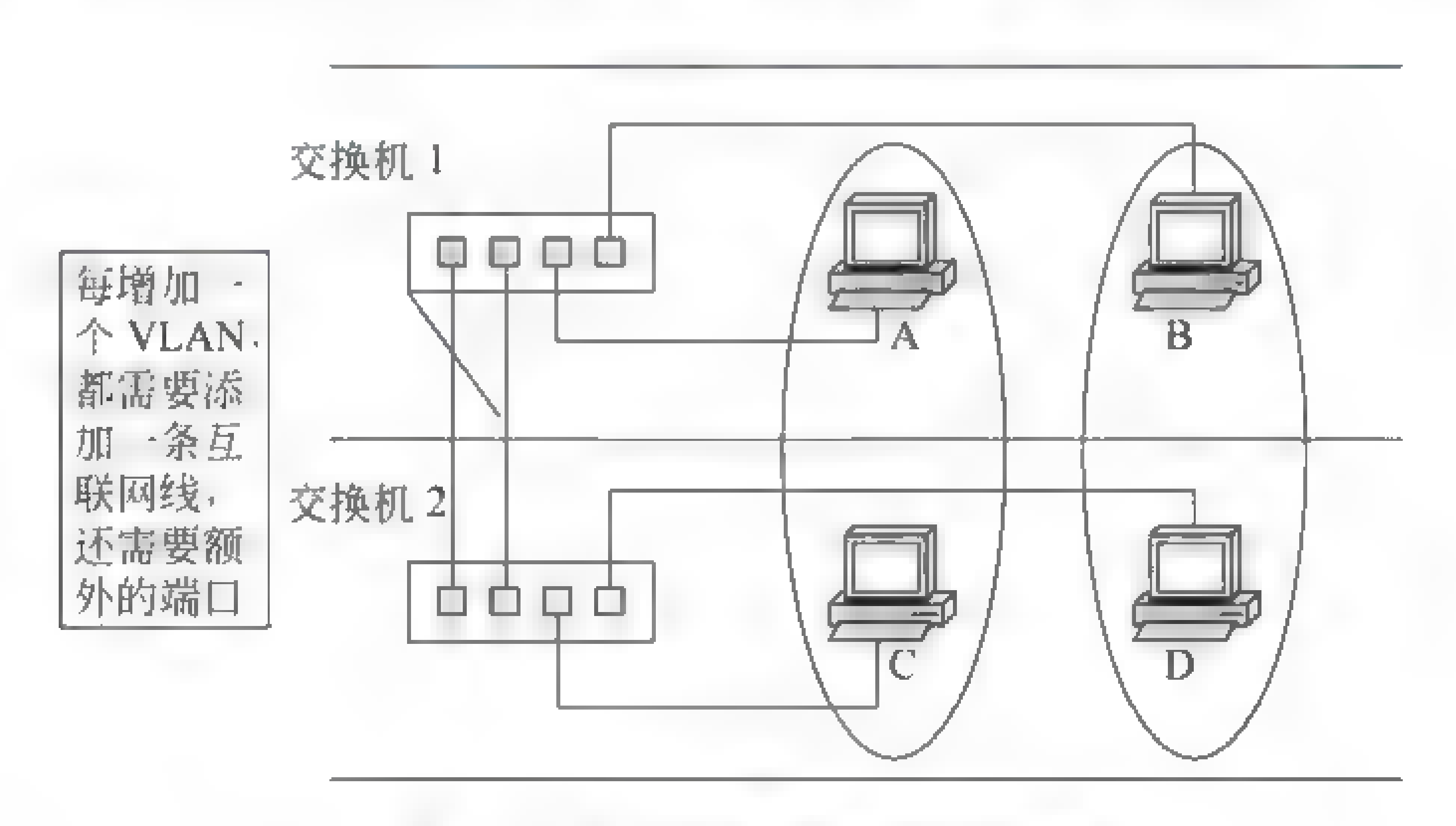


图 2-6 两台交换机的简单连接

这个办法从扩展性和管理效率来看都不好。例如，在现有网络基础上新建 VLAN 时，为了让这个 VLAN 互通，需要在交换机间连接新的网线。建筑物楼层间的纵向布线是比较麻烦的，一般不能由基层管理人员随意操作，而且，VLAN 越多，楼层间（严格地说是交换机间）互联所需的端口越多。交换机端口的利用效率低是对资源的浪费，也限制了网络的扩展。

为了避免这种低效率的连接方式，人们想办法让交换机间互联的网线集中到一根上，这时使用的就是汇聚链接的方法。

2. 汇聚链接

汇聚链接（Trunk Link）指的是能够转发多个不同 VLAN 的通信的端口。汇聚链路

上流通的数据帧都被附加了用于识别分属于哪个 VLAN 的特殊信息。

考虑图 2-7 所示网络，如果采用汇聚链路，用户只需要简单地将交换机间互联的端口设定为汇聚链接就可以了。这时使用的网线还是普通的 UTP 线，而不是其他特殊布线。

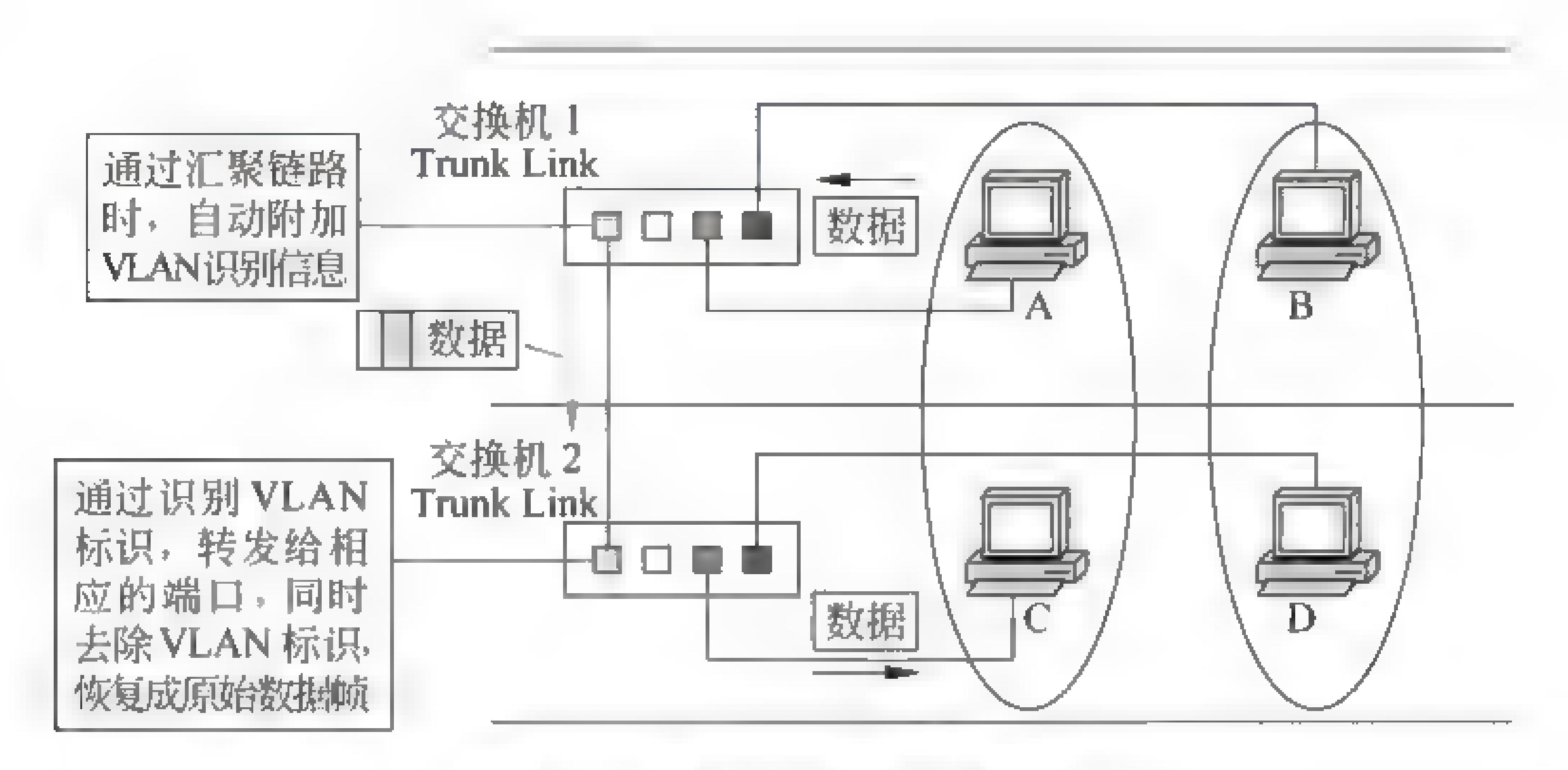


图 2-7　交换机之间的汇聚链接

3. 汇聚链接的方法

下面讨论汇聚链接是如何实现跨越多台交换机的 VLAN。

计算机 A 发送的数据帧从交换机 1 经过汇聚链路到达交换机 2 时，在数据帧上附加了表示属于 VLAN 1 的标记。

交换机 2 收到数据帧后，经过检查 VLAN 标识，发现这个数据帧是属于 VLAN 1 的，因此，去除标记后，根据需要将复原的数据帧只转发给其他属于 VLAN 1 的端口。这时的转发是指经过确认目标 MAC 地址并与 MAC 地址列表比对后只转发给目标 MAC 地址所连的端口。只有当数据帧是一个广播帧、多播帧或是目标不明的帧时，它才会被转发到所有属于 VLAN 1 的端口，如图 2-7 所示。

VLAN 2 发送数据帧时的情形与此相同。

通过汇聚链路时附加的 VLAN 识别信息有可能支持标准的 IEEE 802.1q 协议，也可能是 Cisco 产品独有的 ISL(Inter Switch Link)。如果交换机支持这些规则，用户就能够高效率地构筑横跨多台交换机的 VLAN。

另外，汇聚链路上流通着多个 VLAN 的数据，自然负载较重。因此，在设定汇聚链接时，一个前提是必须支持 100Mbps 以上的传输速度。

在默认条件下，汇聚链接会转发交换机上存在的所有 VLAN 的数据。换一个角度看，可以认为汇聚链接(端口)同时属于交换机上所有的 VLAN。由于实际应用中很可能并不需要转发所有 VLAN 的数据，因此为了减轻交换机的负载，也为了减少对带宽的浪费，可以通过用户设定限制能够经由汇聚链路互联的 VLAN。

4. IEEE 802.1q 与 ISL

在交换机的汇聚链接上，可以通过对数据帧附加 VLAN 信息，构建跨越多台交换机

的 VLAN。

对于附加 VLAN 信息的方法，最具有代表性的是 IEEE 802.1q 和 ISL。下面讨论这两种协议分别如何对数据帧附加 VLAN 信息。

(1) IEEE 802.1q

IEEE 802.1q 俗称"Dot One q"，是经过 IEEE 认证的对数据帧附加 VLAN 识别信息的协议。IEEE 802.1q 所附加的 VLAN 识别信息位于数据帧中"发送源 MAC 地址"与"类别域(Type Field)"之间，具体内容为 2 字节的 TPID 和 2 字节的 TCI，共计 4 字节，如图 2-8 所示。

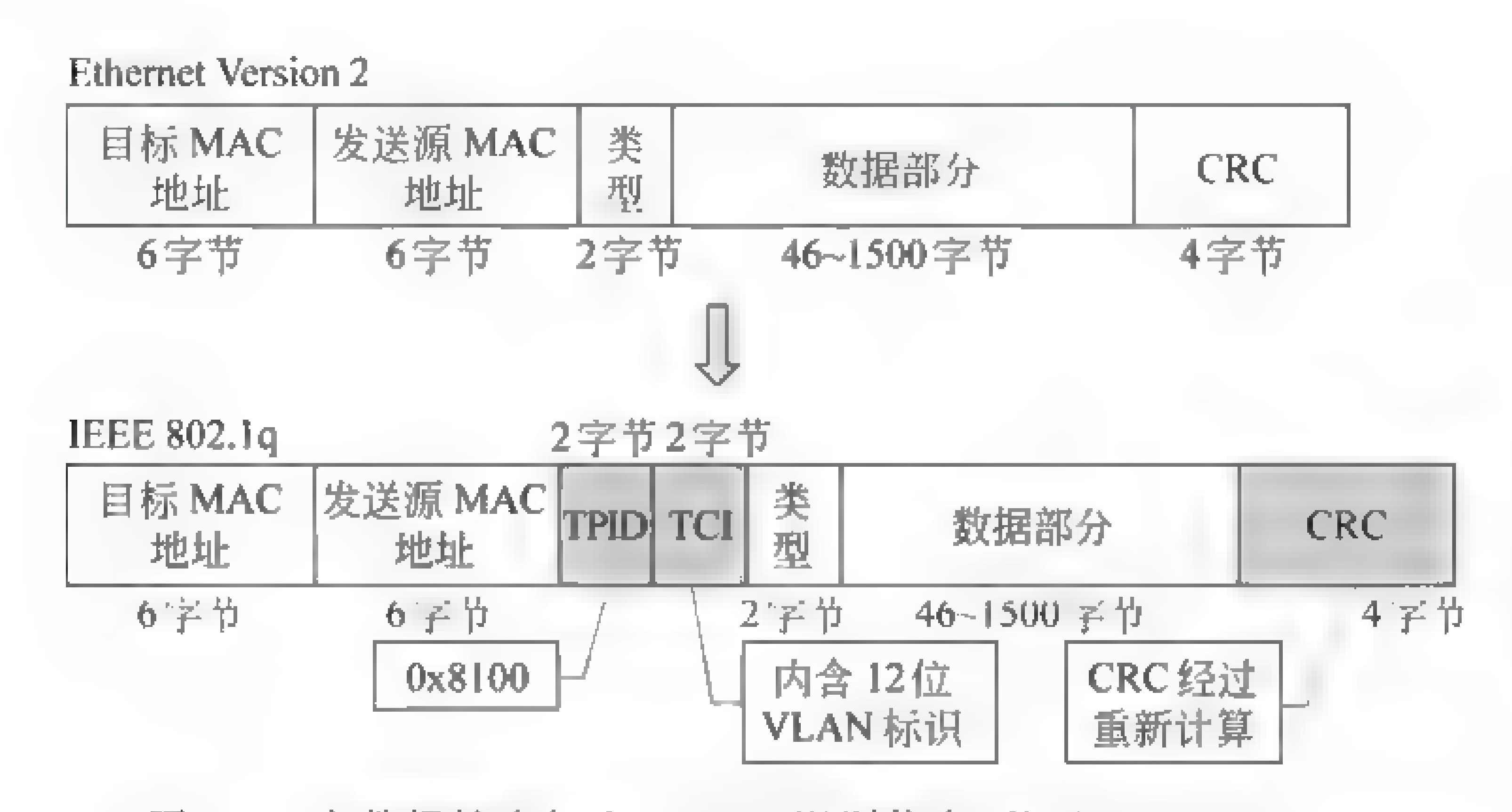


图 2-8　在数据帧中加入 VLAN 识别信息(基于 IEEE 802.1q)

在数据帧中添加了 4 字节内容，CRC 值自然有所变化。这时，数据帧上的 CRC 是插入 TPID 和 TCI 后，对包括它们在内的整个数据帧重新计算后所得的值。

当数据帧离开汇聚链路时，TPID 和 TCI 会被去除，这时要重新计算一次 CRC。

TPID 的值固定为 0x8100。交换机通过 TPID 确定数据帧内附加了基于 IEEE 802.1q 的 VLAN 信息。而实质上的 VLAN ID 是 TCI 中的 12 位，由于总共有 12 位，因此最多可识别 4096 个 VLAN。

基于 IEEE 802.1q 附加的 VLAN 信息就像在传递物品时附加的标签，因此也称为"标签型 VLAN(Tagging VLAN)"。

(2) ISL

ISL(Inter Switch Link)是 Cisco 产品支持的一种与 IEEE 802.1q 类似的用于在汇聚链路上附加 VLAN 信息的协议。使用 ISL 后，每个数据帧头部都会被附加 26 字节的"ISL 包头(ISL Header)"，并且在帧尾带上通过对包括 ISL 包头在内的整个数据帧进行计算后得到的4 字节 CRC 值。换言之，总共增加了 30 字节信息，如图 2-9 所示。

在使用 ISL 的环境下，当数据帧离开汇聚链路时，只要简单地去除 ISL 包头和新 CRC 就可以了。由于原先的数据帧及其 CRC 都被完整保留，因此无须重新计算 CRC。

ISL 有如用 ISL 包头和新 CRC 将原数据帧整个包裹起来，因此称为"封装型 VLAN(Encapsulated VLAN)"。

需要注意的是，不论是 IEEE 802.1q 的"Tagging VLAN"，还是 ISL 的"Encapsulated

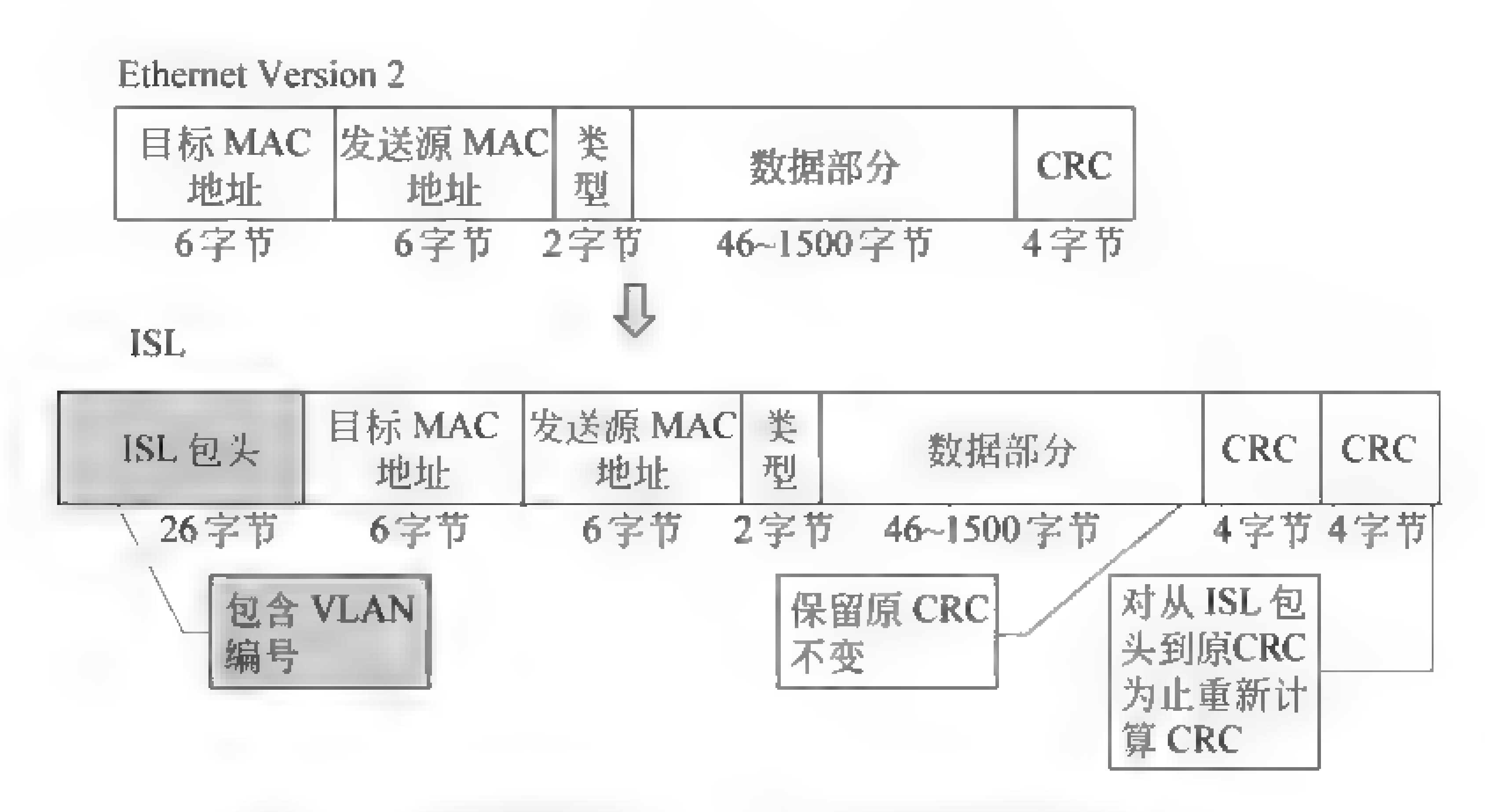


图 2-9 在数据帧中加入 VLAN 识别信息(基于 ISL)

VLAN",都不是很严格的称谓。在不同的书籍与参考资料中,上述词语有可能被混合使用,大家在学习时要格外注意。由于 ISL 是 Cisco 独有的协议,因此只能用于 Cisco 网络设备之间的互联。

5. 配置实例

ThreeFour Software 公司有两个主要部门:销售部和技术部,其中销售部门的个人计算机系统分散连接在不同楼层的两台交换机上,部门内部之间需要相互通信,如何在交换机上做适当配置来实现这一目标呢?构建如图 2-10 所示网络结构,其配置过程如下:

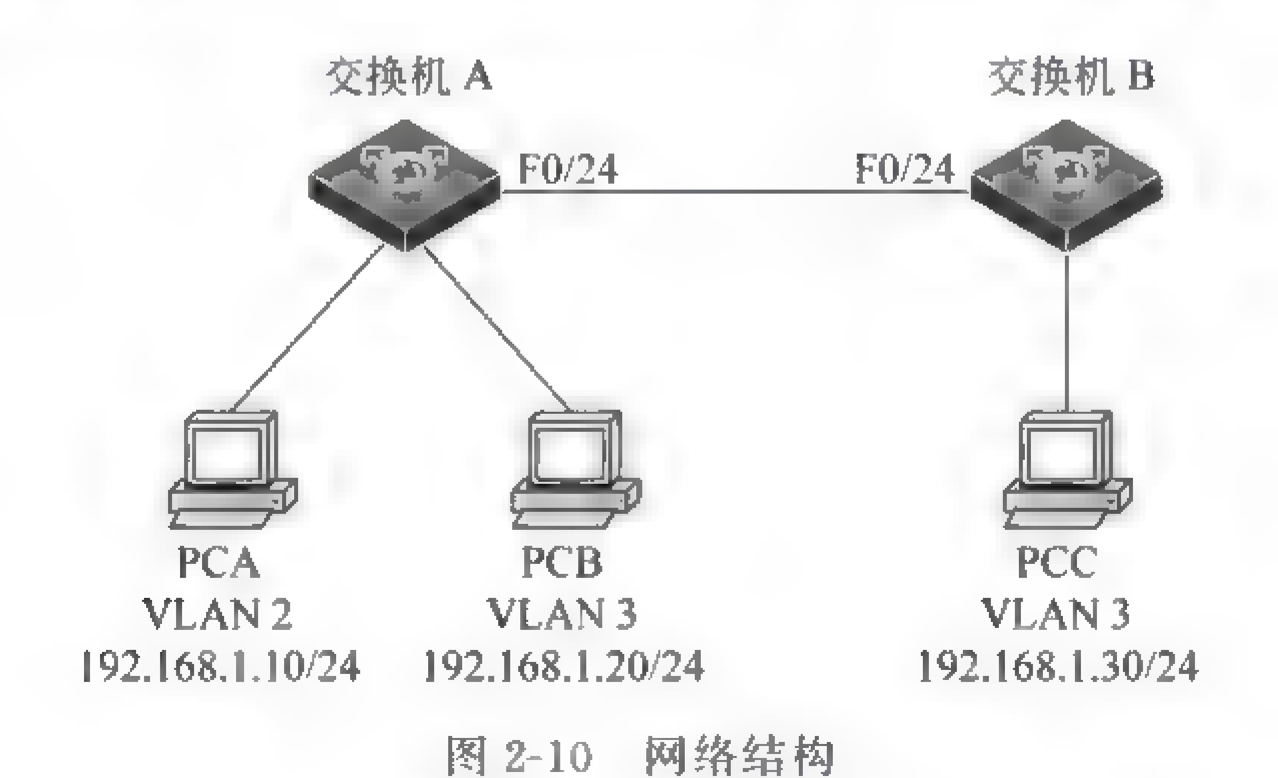


图 2-10 网络结构

① 在交换机 SwitchA 上创建 vlan 2,并将 0/9 端口划分到 vlan 2 中。

```
SwitchA# conf ter
SwitchA(config)# valn 2
SwitchA(config-vlan)# name jjj
SwitchA(config-vlan)# exit
SwitchA(config)# int fast0/9
SwitchA(config-if)# swit acc vlan 2
```

② 在交换机 SwitchA 上创建 vlan 3,并将 0/12 端口划分到 vlan 3 中。

```
SwitchA(config)#vlan 3
SwitchA(config vlan)#name qep
SwitchA(config-vlan)#exit
SwitchA(config)#int fast0/12
SwitchA(config-if)#swit acc vlan 3
```

③ 把交换机 SwitchA 与 SwitchB 相连的端口(通常为 0/24 端口)定义为 tag vlan 模式(trunk)。

```
SwitchA(config)#int fast0/24
SwitchA(config-if)#swit mode trunk
```

④ 在交换机 SwitchB 上创建 vlan 3,并将 0/9 端口划分到 vlan 3 中。

```
SwitchB# conf ter
SwitchB(config)#valn 3
SwitchB(config-vlan)#name jjj
SwitchB(config-vlan)#exit
SwitchB(config)#int fast0/9
SwitchB(config-if)#swit acc vlan 3
```

⑤ 把 SwitchB 连接的端口(通常为 0/24 端口)定义为 tag vlan 模式。

```
SwitchB(config)#int fast0/24
SwitchB(config-if)#swit mode trunk
```

⑥ 用 ping 测试。

2.3.2 VLAN 间路由(不同 VLAN 通信)

1. VLAN 间路由的必要性

根据所学的知识我们知道,两台计算机即使连接在同一台交换机上,只要所属的 VLAN 不同,就无法直接通信。接下来将介绍如何在不同的 VLAN 间进行路由,使分属不同 VLAN 的主机能够互相通信。

首先回顾为什么不同 VLAN 间不通过路由就无法通信。要在 LAN 内通信,必须在数据帧头中指定通信目标的 MAC 地址。为了获取 MAC 地址,TCP/IP 协议下使用的是 ARP。ARP 解析 MAC 地址是要通过广播。也就是说,如果广播报文无法到达,就无从解析 MAC 地址,无法直接通信。

计算机分属不同的 VLAN,也就意味着分属不同的广播域,自然收不到彼此的广播报文。因此,属于不同 VLAN 的计算机之间无法直接通信。为了能够在 VLAN 间通信,需要利用 OSI 参考模型中更高的一层——网络层信息(IP 地址)进行路由。关于路由的具体内容,将在后面章节中详细介绍。

路由功能主要由路由器提供。在今天的局域网里经常利用带有路由功能的交换机——三层交换机(Layer 3 Switch)来实现。下面将介绍使用路由器和三层交换机进行 VLAN 间路由的情况。

在使用路由器进行 VLAN 间路由时，与构建横跨多台交换机的 VLAN 时的情况类似，还是会遇到“该如何连接路由器与交换机”这个问题。路由器和交换机的接线方式大致有两种，一种是将路由器与交换机上的每个 VLAN 分别连接；另一种是不论 VLAN 有多少个，路由器与交换机都只用一条网线连接。

最容易想到的，当然是把路由器和交换机以 VLAN 为单位分别用网线连接。即将交换机上用于和路由器互联的每个端口设为访问链接，然后分别用网线与路由器上的独立端口互联。如图 2-11 所示，交换机上有 2 个 VLAN，就需要在交换机上预留 2 个端口用于与路由器互联，在路由器上同样需要有 2 个端口，两者之间用 2 条网线分别连接。

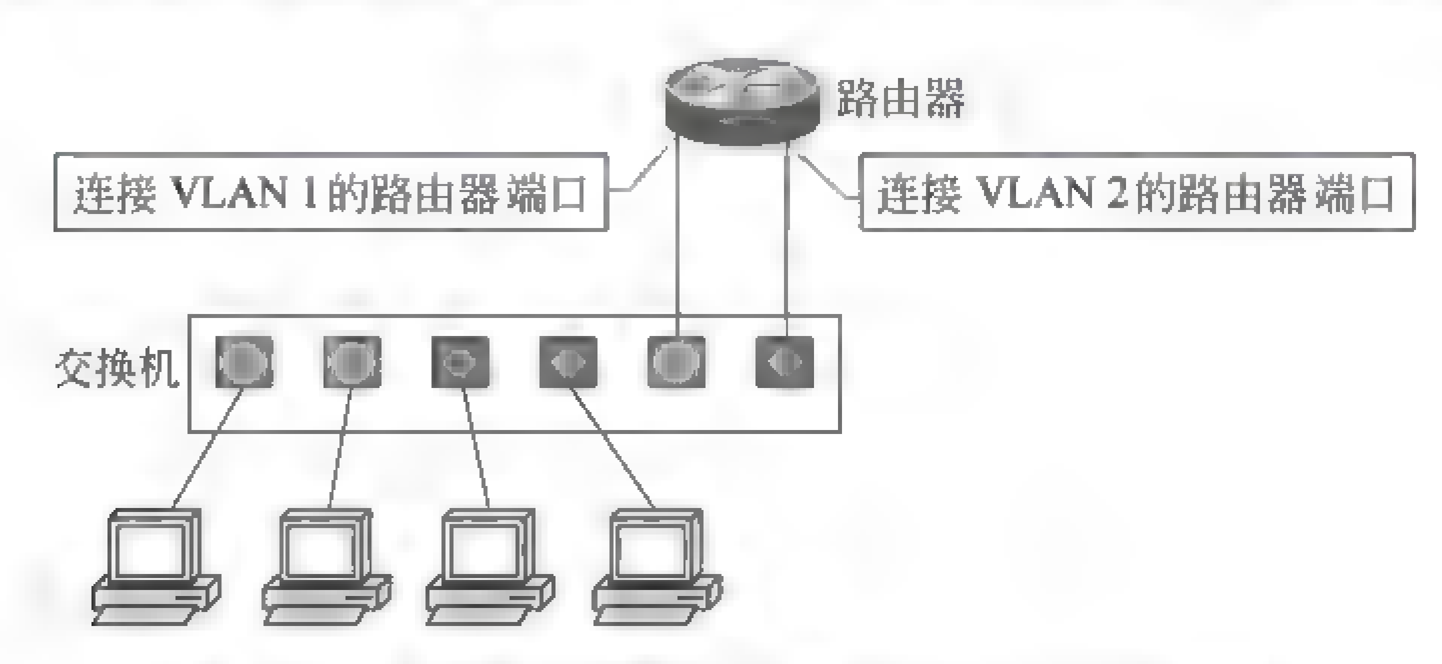


图 2-11　路由器与交换机上的每个 VLAN 分别连接

采用这种办法，其扩展性很成问题。每增加一个新的 VLAN，都需要消耗路由器的端口和交换机上的访问链接，还需要重新布设一条网线。而路由器通常不会带有太多 LAN 接口。新建 VLAN 时，为了对应增加的 VLAN 所需的端口，必须将路由器升级成带有多个 LAN 接口的高端产品，这部分成本以及重新布线的开销都使得这种接线法不受欢迎。

那么，第二种办法“不论 VLAN 有多少个，路由器与交换机都只用一条网线连接”是如何做的呢？当使用一条网线连接路由器与交换机进行 VLAN 间路由时，需要用到汇聚链接，其具体实现过程为：首先，将用于连接路由器的交换机端口设为汇聚链接，路由器上的端口也必须支持汇聚链路。双方用于汇聚链路的协议必须相同。其次，在路由器上定义对应各个 VLAN 的子接口(Sub-Interface)。尽管实际与交换机连接的物理端口只有一个，但在理论上可以把它分割为多个虚拟端口，如图 2-12 所示。

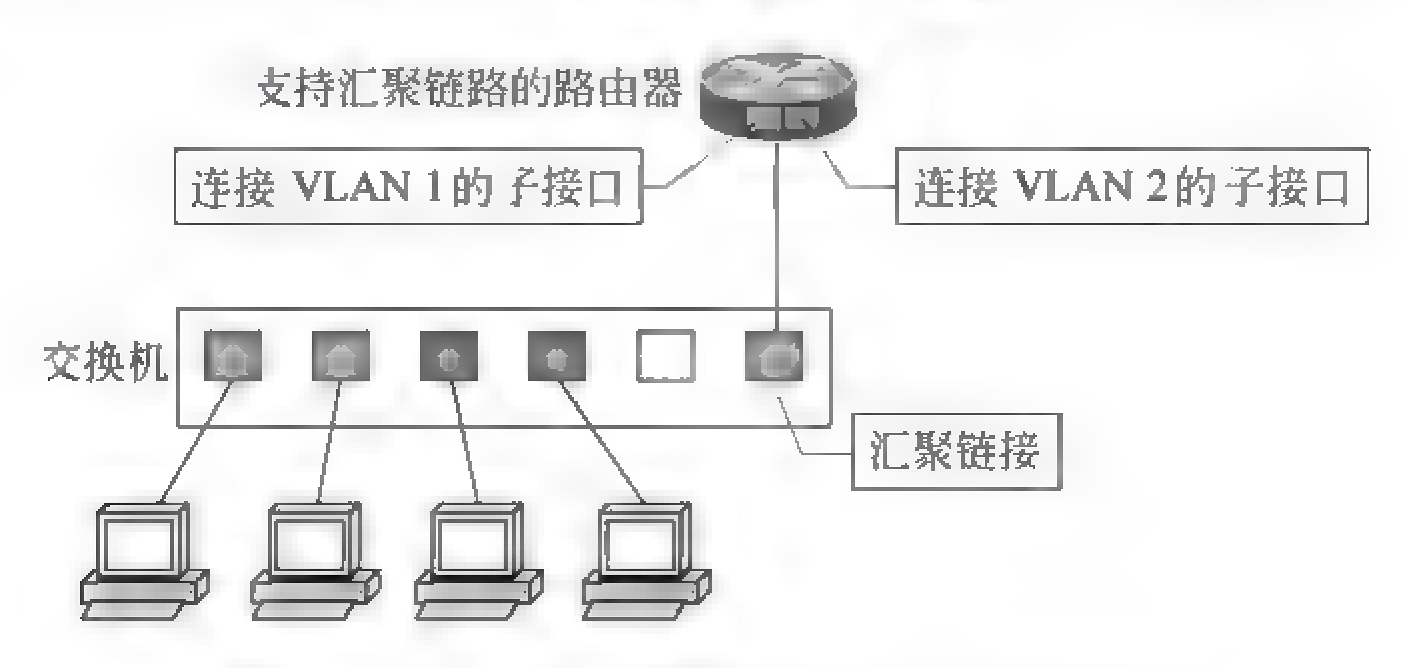


图 2-12　路由器与交换机只用一条网线连接

VLAN 将交换机从逻辑上分割成多台交换机，因而用于 VLAN 间路由的路由器必须拥有对应各个 VLAN 的虚拟接口。

采用这种方法，即使以后在交换机上新建 VLAN，仍只需要一条网线连接交换机和路由器。用户只需要在路由器上新设一个对应新 VLAN 的子接口就可以了。与前面的方法相比，其扩展性强得多，也不需要升级 LAN 接口数不足的路由器或重新布线。

2. 同一 VLAN 内的通信

下面介绍使用汇聚链路连接交换机与路由器时，VLAN 间如何路由。如图 2-13 所示，为各台计算机以及路由器的子接口设定 IP 地址。

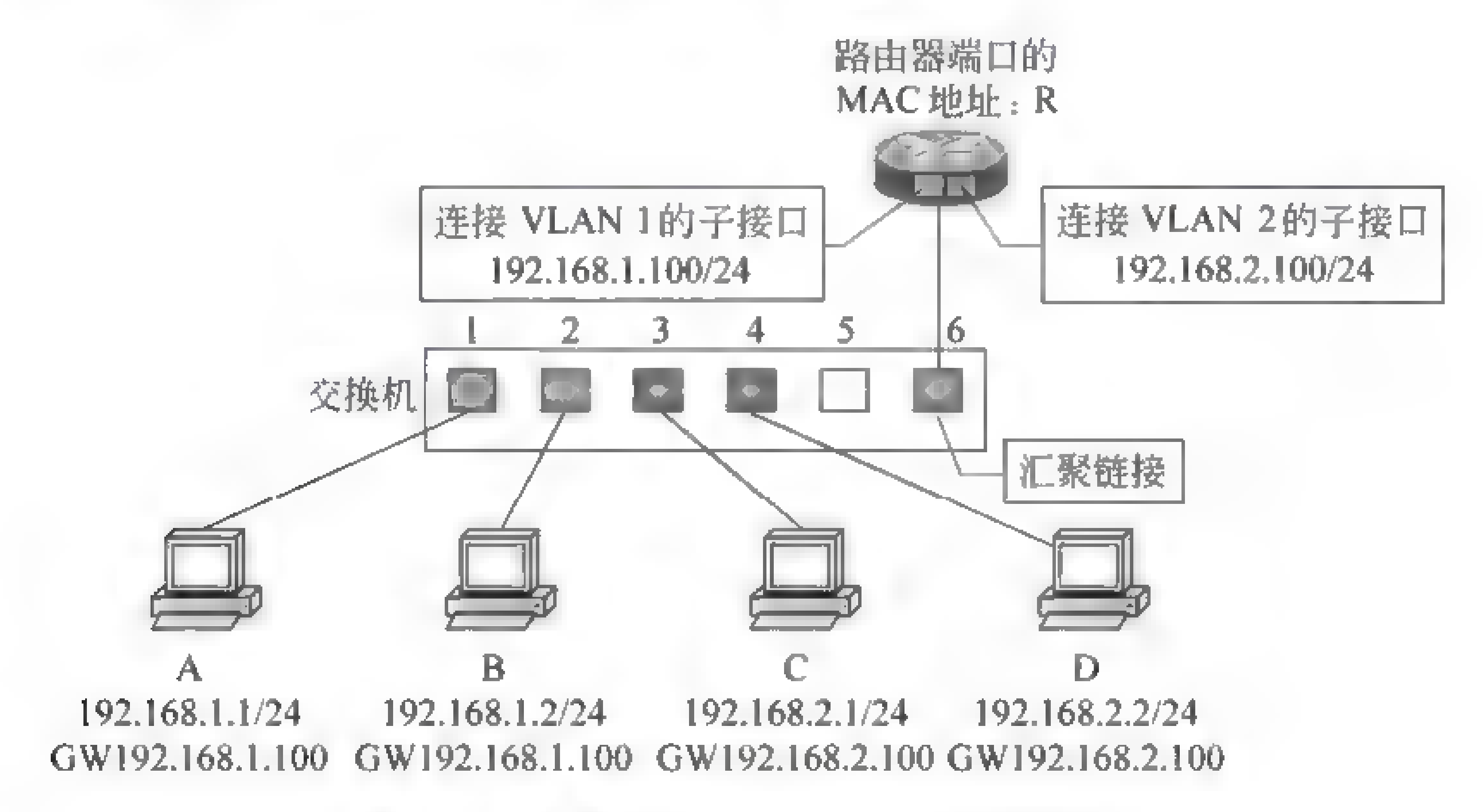


图 2-13　设置对应各个 VLAN 的虚拟接口

VLAN 1(VLAN ID=1)的网络地址为 192.168.1.0/24，VLAN 2(VLAN ID=2)的网络地址为 192.168.2.0/24。各台计算机的 MAC 地址分别为 A，B，C，D，路由器汇聚链接端口的 MAC 地址为 R。交换机通过对各端口所连计算机 MAC 地址的学习，生成一个 MAC 地址列表。

首先考虑计算机 A 与同一 VLAN 内的计算机 B 之间通信的情形。计算机 A 发出 ARP 请求信息，请求解析 B 的 MAC 地址。交换机收到数据帧后，检索 MAC 地址列表中与收信端口同属一个 VLAN 的表项。结果发现计算机 B 连接在端口 2 上，于是交换机将数据帧转发给端口 2，最终计算机 B 收到该帧。对于收、发信双方同属一个 VLAN 的通信，一切处理均在交换机内完成。如图 2-14 所示。

3. 不同 VLAN 间通信时数据的流程

考虑计算机 A 与计算机 C 之间通信的情况。计算机 A 从通信目标的 IP 地址(192.168.2.1)得出计算机 C 与本机不属于同一个网段，因此向设定的默认网关(Default Gateway)转发数据帧。在发送数据帧之前，需要先用 ARP 获取路由器的 MAC 地址。

交换机得到路由器的 MAC 地址 R 后，将按图 2-15 所示的步骤向 C 发送数据帧。图

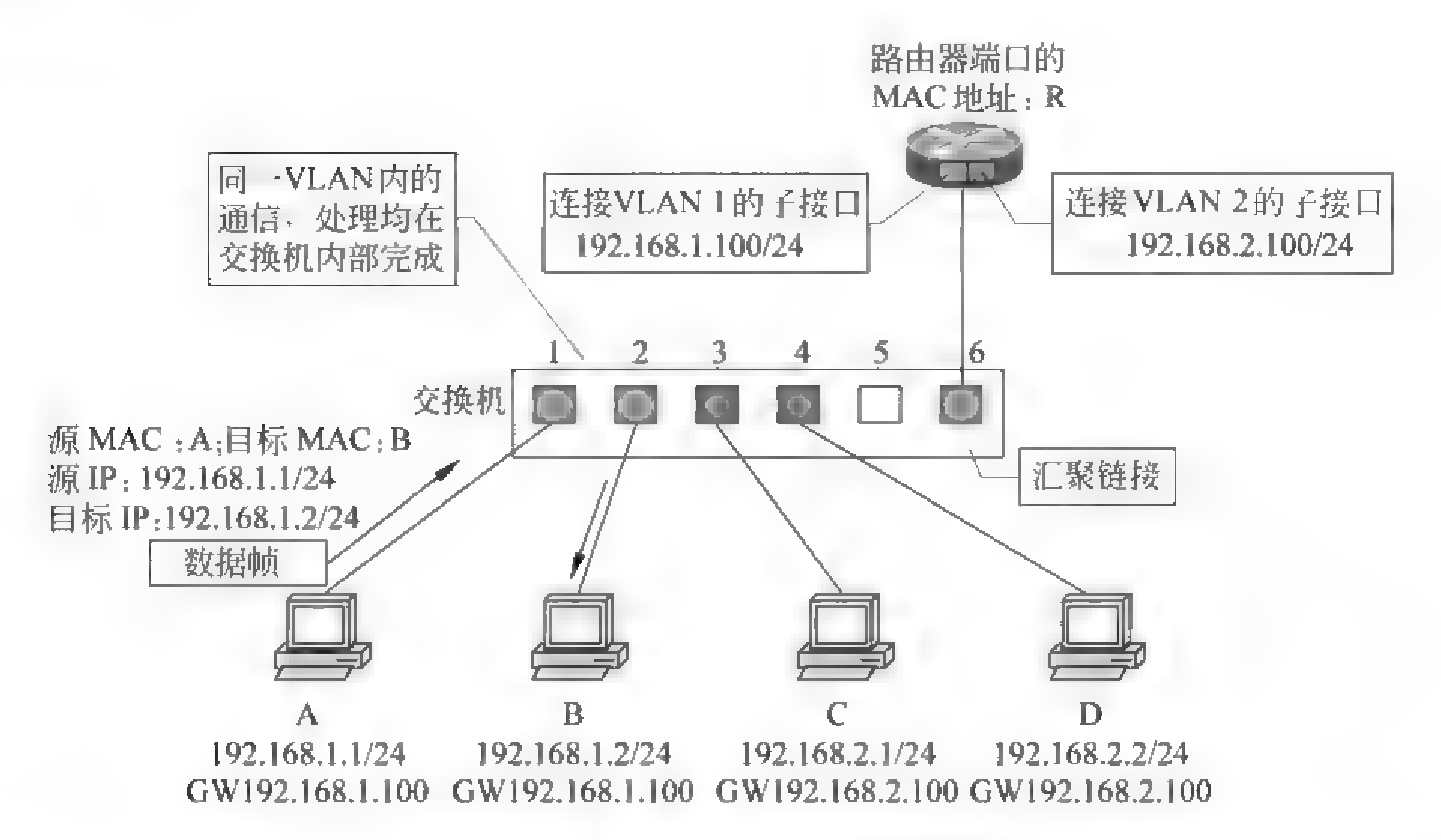


图 2-14　同一 VLAN 中的数据传输

中，在①的数据帧中，目标 MAC 地址是路由器的地址 R，内含的目标 IP 地址仍是最终的通信对象 C 的地址。这一部分内容涉及局域网内经过路由器转发的步骤。

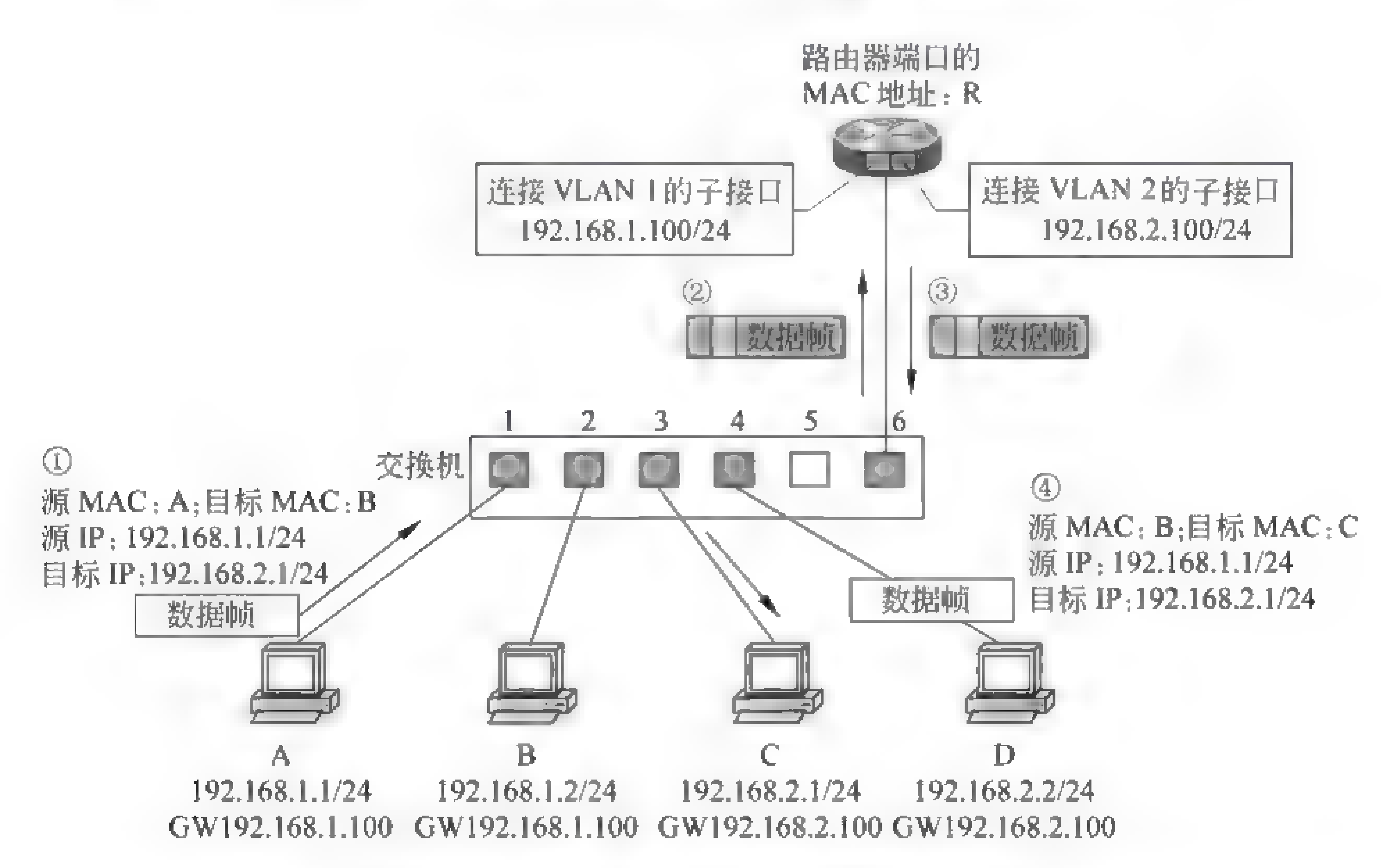


图 2-15　不同 VLAN 间通信时数据的流程

交换机在端口 1 上收到①的数据帧后，检索 MAC 地址列表中与端口 1 同属一个 VLAN 的表项。由于汇聚链路会被看做属于所有的 VLAN，因此这时交换机的端口 6 也属于被参照对象。这样，交换机就知道往 MAC 地址 R 发送数据帧，需要经过端口 6 转发。

从端口 6 发送数据帧时，由于它是汇聚链接，会被附加 VLAN 识别信息。由于是来自 VLAN 1 的数据帧，因此如图 2-15 中②所示，会被加上 VLAN 1 的识别信息后进入汇

聚链路。路由器收到②的数据帧后，确认其 VLAN 识别信息，由于它是属于 VLAN 1 的数据帧，因此交由负责红色 VLAN 的子接口接收。

接着，根据路由器内部的路由表判断该向哪里转发。

由于目标网络 192.168.2.0/24 是 VLAN 2，且该网络通过子接口与路由器直连，因此只要从负责 VLAN 2 的子接口转发就可以了。这时，数据帧的目标 MAC 地址被改写成计算机 C 的目标地址，并且由于需要经过汇聚链路转发，因此被附加了属于 VLAN 2 的识别信息。这就是图中③的数据帧。

交换机收到③的数据帧后，根据 VLAN 标识信息从 MAC 地址列表中检索属于 VLAN2 的表项。由于通信目标计算机 C 连接在端口 3 上，并且端口 3 为普通的访问链接，因此交换机将数据帧除去 VLAN 识别信息后（数据帧④）转发给端口 3，使计算机 C 成功地收到这个数据帧。

VLAN 间通信时，即使通信双方连接在同一台交换机上，也必须经过“发送方—交换机—路由器—交换机—接收方”这样一个流程。

任务 2.4　交换网络中的冗余链路管理

随着交换技术在网络中的普遍应用，保证各种网络终端（包括服务器）设备间正常通信成为一项重要的任务。在绝大多数情况下，在交换设备之间用多条链路连接，形成冗余链路，以保证线路上的单点故障不会影响正常的网络通信。但交换机的基本工作原理导致这样的设计会在交换网络中产生严重的广播风暴。本节将介绍在交换网络中既能保证冗余链路提供链路备份，又避免广播风暴的技术——生成树技术。

2.4.1　交换机网络中的冗余链路

在由许多交换机或交换设备组成的网络环境中通常使用一些备份连接，以提高网络的健壮性和稳定性。备份连接也叫备份链路、冗余链路。备份链路如图 2-16 所示，交换机 SW1 与交换机 SW3 的端口 1 之间的链路就是一条备份连接。在主链路（交换机 SW1 与 SW2 的端口 2 之间的链路，或者交换机 SW2 的端口 1 与交换机 SW3 的端口 2 之间的链路）出现故障时，备份链路自动启用，提高了网络的整体可靠性。

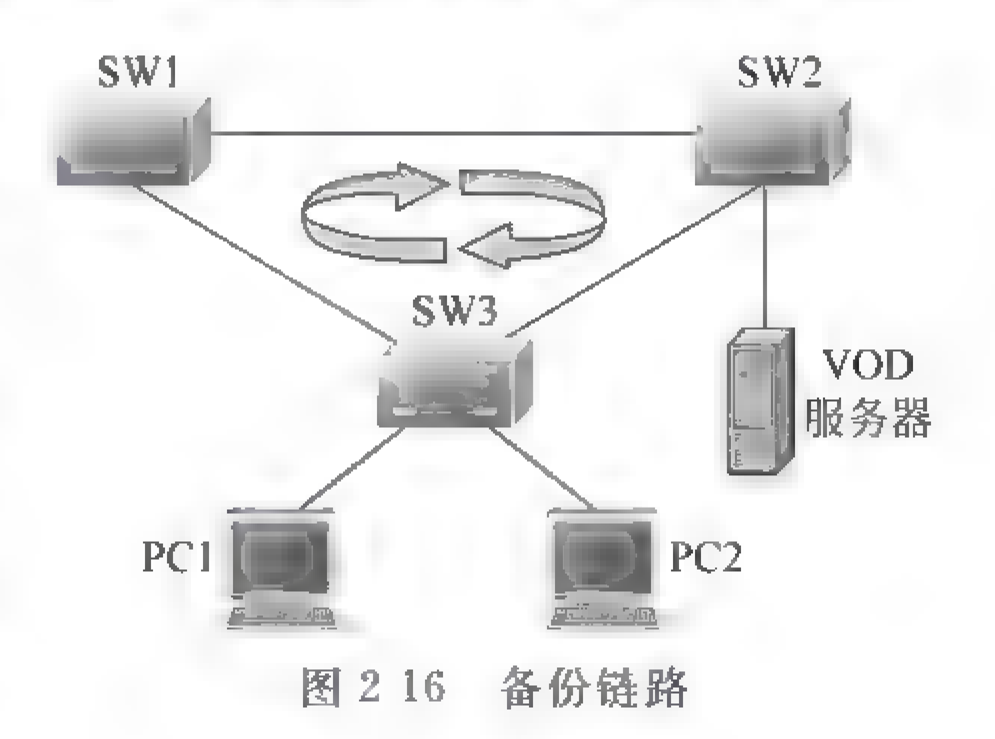


图 2-16　备份链路

使用冗余备份能够提高网络的健壮性、稳定性和可靠性，但是备份链路使网络存在环路。在图 2-16 中，SW1—SW2—SW3 就是一个环路。环路是备份链路面临的最严重的问题，将导致广

播风暴、多帧复制以及不稳定的 MAC 地址表等。

2.4.2 以太网链路聚合

1. 网络压力

对于局域网交换机之间以及从交换机到高需求服务的许多网络连接来说，100Mbps 甚至 1Gbps 的带宽是不够的。链路聚合（也称为端口聚合）技术帮助用户减小了这种压力。

IEEE 802.3ad 标准定义了如何将两条以上的以太网链路组合起来，为高带宽网络连接提供负载共享、负载平衡以及更好的弹性。端口聚合将交换机上的多个端口在物理上连接起来，在逻辑上捆绑在一起，成为一个拥有较大带宽的端口，形成一条干路，实现负载均衡，并提供冗余链路。

端口聚合（AP，Aggregate Port）符合 IEEE 802.3ad 标准，它把多个端口的带宽叠加起来使用，如图 2-17 所示。比如，全双工快速以太网端口形成的 AP 最大可以达到 800Mbps，或者千兆以太网接口形成的 AP 最大可以达到 8Gbps。

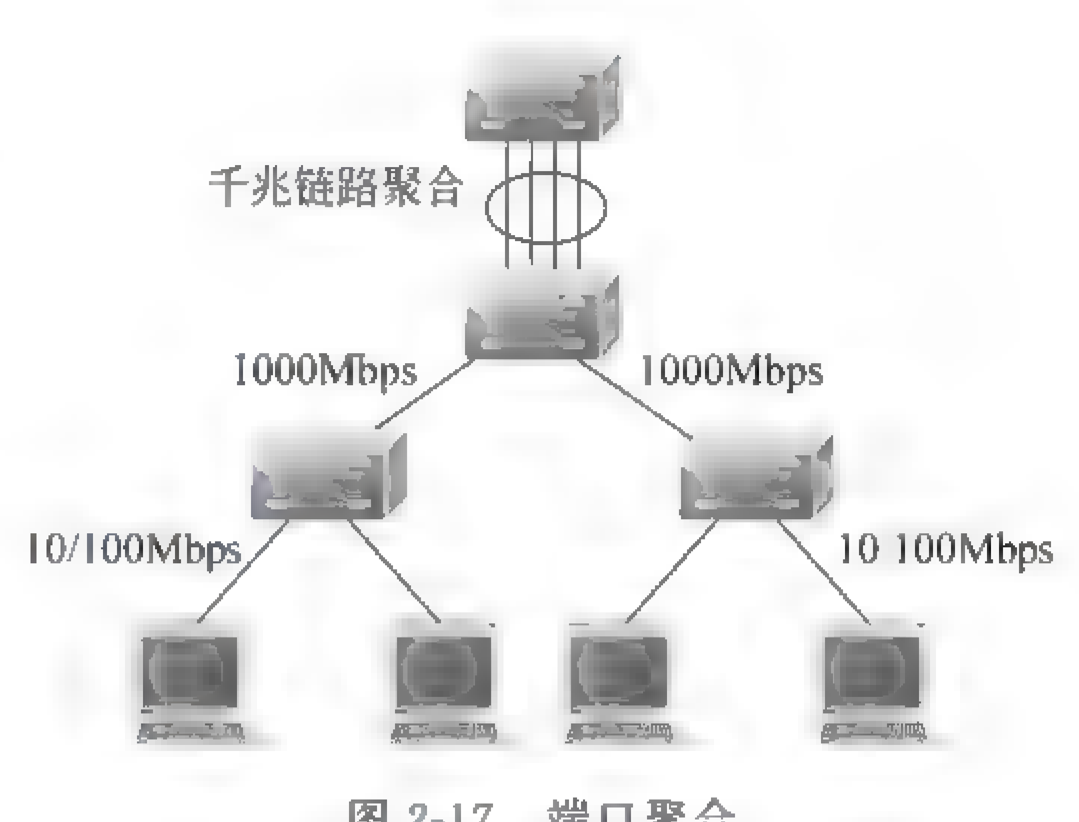


图 2-17 端口聚合

IEEE 802.3ad 的主要优点如下：

① 链路聚合技术（也称端口聚合）帮助用户减少网络带宽不足的压力。

② 具有可靠性。

③ 链路聚合标准在点到点链路上提供了固有的、自动的冗余性。

2. 流量平衡

AP 根据报文的 MAC 地址或 IP 地址进行流量平衡，即把流量平均地分配到 AP 的成员链路中。流量平衡可以根据源 MAC 地址/目的 MAC 地址或源 IP 地址/目的 IP 地址对来完成。

3. 配置 AP

(1) 配置二层 AP

可以通过全局配置模式下的 interface aggregateport 命令手动创建一个 AP。无论二、三层物理接口如何，当把接口加入一个不存在的 AP 时，AP 会被自动创建。无论二、三层物理接口如何，都可以使用接口配置模式下的 port group 命令加入一个 AP。

用户可以使用接口配置模式下的 port group 命令，将一个以太网接口配置成一个 AP 的成员口。从特权模式出发，按以下步骤将以太网接口配置成一个 AP 接口的成

员口：

```
Switch# configure terminal
Switch(config) #interface interface-id                !选择端口,进入接口配置模式
Switch(config-if)#port-group port-group-number
                                   !将该接口加入一个 AP(如果这个 AP 不存在,则同时创建该 AP)。
Switch(config-if-range)#end                           !回到特权模式
```

在接口配置模式下使用 no port-group 命令将删除一个 AP 成员接口。

下面的例子是将二层以太网接口 0/1 和 0/2 配置成二层 AP 5 成员。

```
Switch# configure terminal
Switch(config)# interface range fastethernet 0/1-2
Switch(config-if-range)#port-group 5
Switch(config-if-range)#end
```

可以在全局配置模式下使用命令 interface aggregatepor n(n 为 AP 号)来直接创建一个 AP(如果 AP n 不存在)。

(2) 配置三层 AP

默认情况下,AP 是二层的,如果要配置三层 AP,需要进行下面的操作。

从特权模式出发,按以下步骤配置三层 AP 接口：

```
Switch# configure terminal
Switch(config) #interface aggregate-port aggregate-port-number      !创建一个 AP
Switch(config-if)#no switchport                       !将该接口设置为三层模式
Switch(config-if)#ip address ip-address mask          !给 AP 配置 IP 地址和子网掩码
Switch(config-if)#end
```

下面的例子是配置一个三层 AP(AP3)并给它配置 IP 地址(192.168.1.1)。

```
Switch# configure terminal
Switch(config) #interface aggregate-port 3
Switch(config-if)#no switchport
Switch(config-if)#ip address 192.168.1.1 255.255.255.0
Switch(config-if)#end
```

(3) 配置 AP 的流量平衡算法

```
Switch(config) #aggregateport load-balance {dst-mac |src-mac |ip}
```

其中,dst mac 是根据报文的目的 MAC 地址进行流量分配;src mac 是根据报文的源 MAC 地址进行流量分配;ip 是根据源 IP 与目的 IP 进行流量分配。在三层条件下,建议采用此流量平衡方式。

要将 AP 的流量平衡设置恢复到默认值,可以在全局配置模式下使用 no aggregateport load balance 命令。

(4) 显示 aggregate port

可以在特权模式下显示 AP 设置。

```
show aggregateport [port number]{load balance| summary}
```

(5) 配置 AP 的注意事项

① 组端口的速度必须一致；

② 组端口必须属于同一个 VLAN；

③ 组端口使用的传输介质相同；

④ 组端口必须属于同一层次，并与 AP 在同一层次。

任务 2.5 配置生成树协议（STP/RSTP）

在由交换机构成的交换网络中通常设计有冗余链路和设备。这种设计的目的是防止一个点的失败导致整个网络功能的丢失。虽然冗余设计可能消除单点失败问题，但导致了交换回路的产生，带来了如下问题：广播风暴、多帧复制和地址表不稳定。因此，在交换网络中必须有一个机制来阻止回路，生成树协议(Spanning Tree Protocol)的作用正在于此。

生成树协议定义在 IEEE 802.1d 中，是一种桥到桥的链路管理协议，它在防止产生自循环的基础上提供路径冗余，因此其主要作用是避免回路，冗余备份。为使以太网更好地工作，两个工作站之间只能有一条活动路径。网络环路的发生有多种原因，最常见的是故意生成的冗余，一条链路或交换机失败，会有另一条链路或交换机替代。

生成树协议的主要思想就是当网络中存在备份链路时，只允许主链路激活；如果主链路因故障而被断开后，备用链路才会被打开。

生成树协议划分成三代，即第一代生成树协议 STP/RSTP、第二代生成树协议 PVST/PVST＋和第三代生成树协议 MISTP/MSTP。

2.5.1 生成树协议工作原理

1. 生成树协议简介

生成树协议的使用基于以下几点：

① 有一个唯一的组地址(01 80 C2 00 00 00)标识一个特定 LAN 上的所有交换机。这个组地址能被所有的交换机识别。

② 每台交换机有一个唯一的标识(Bridge Identifier)。

③ 每台交换机的端口有一个唯一的端口标识(Port Identifier)。

对生成树的配置进行管理还需要对每台交换机调协一个相对的优先级；对每台交换机的每个端口调协一个相对的优先级；对每个端口调协一个路径花费。

具有最高优先级的交换机称为根(root)交换机。每台交换机端口都有一个根路径花费，根路径花费是该交换机到根交换机所经过的各个路段的路径花费的总和。在一台交换机中，根路径花费的值最低的端口称为根端口。若有多个端口具有相同的根路径花费，则具有最高优先级的端口为根端口。

在每个 LAN 中都有一台交换机被称为指定(designated)交换机，它是该 LAN 中根路径花费最少的交换机。把 LAN 和指定交换机连接起来的端口就是 LAN 的指定端口(designated port)。如果指定交换机中有两个以上的端口连在这个 LAN 上，则具有最高优先级的端口被选为指定端口，其拓扑结构如图 2-18 所示。

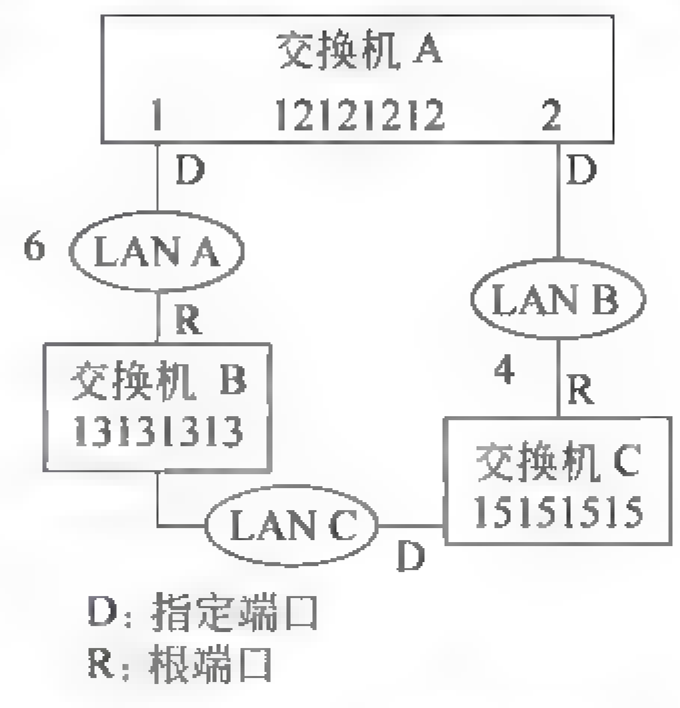


图 2-18　根交换机和根端口

由于交换机 A 具有最高优先级(桥标识最低)，被选为根交换机，所以交换机 A 是 LAN A 和 LAN B 的指定交换机。假设交换机 B 的根路径花费为 6，交换机 C 的根路径花费为 4，那么交换机 C 被选为 LAN C 的指定交换机，即 LAN C 与交换机 A 之间的消息通过交换机 C 转发，而不是通过交换机 B。LAN C 与交换机 B 之间的链路是一条冗余链路。

2. BPDU 编码

交换机之间定期发送 BPDU 包，交换生成树配置信息，以便对网络的拓扑、花费或优先级的变化及时响应。BPDU 分为两种类型，包含配置信息的 BPDU 包称为配置 BPDU (Configuration BPDU)；当检测到网络拓扑结构变化时，要发送拓扑变化通知 BPDU (Topology Change Notification BPDU)。配置 BPDU 编码如图 2-19 所示，拓扑变化通知 BPDU 编码如图 2-20 所示。

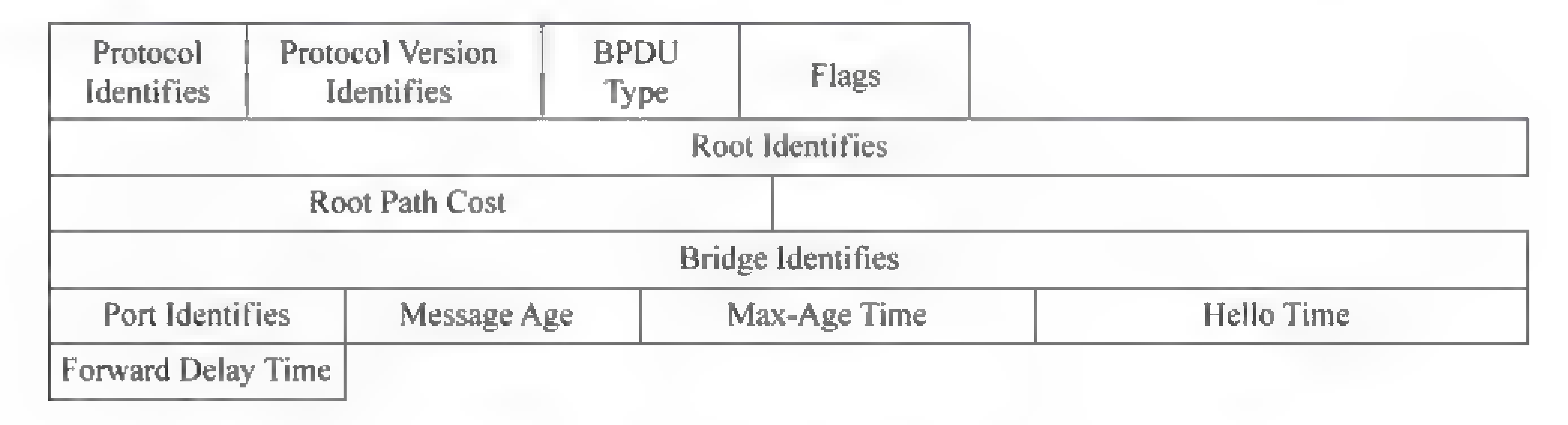


图 2-19　配置 BPDU 编码



图 2-20　拓扑变化通知 BPDU 编码

对于配置 BPDU，超过 35 字节以外的字节将被忽略；对于拓扑变化通知 BPDU，超过 4 字节以外的字节将被忽略。

BPDU 的组成说明如下：

① 版本号：00(IEEE 802.1d)；02(IEEE 802.1w)

② Bridge ID：交换机 ID=交换机优先级+交换机 MAC 地址

③ Root ID：根交换机 ID

④ Root Path Cost：到达根的路径开销
⑤ Port ID：发送 BPDU 的端口 ID=端口优先级+端口编号
⑥ Hello Time：定期发送 BPDU 的时间间隔
⑦ Max-Age Time：保留对方 BPDU 消息的最长时间
⑧ Forward-Delay Time：发送延时，端口状态改变的时间间隔
⑨ 其他表示发现网络拓扑变化、本端口状态的标志位

2.5.2 形成一个生成树所必须决定的要素

1. 决定根交换机

① 交换机的 Bridge ID 由两部分构成：优先级和 MAC 地址；
② 最开始，所有的交换机都认为自己是根交换机；
③ 交换机向与之相连的 LAN 广播发送配置 BPDU，其 root_id 与 bridge_id 的值相同；
④ 当交换机收到另一台交换机发来的配置 BPDU 后，若发现其中 root_id 字段的值大于该交换机中 root_id 参数的值，则丢弃该帧；否则更新该交换机的 root_id、根路径花费 root_path_cost 等参数的值，该交换机将以新值继续广播发送配置 BPDU。

2. 决定根端口

在交换机中，根路径花费的值最低的端口称为根端口。若有多个端口具有相同的最低根路径花费，则具有最高优先级的端口为根端口。若有两个或多个端口具有相同的最低根路径花费和最高优先级，则端口号最小的为默认的根端口。

在生成树的选举过程中，应遵循以下优先顺序来选择最佳路径：
① 比较到达根的路径开销；
② 比较发送者的 Bridge ID；
③ 比较发送者的 Port ID；
④ 比较本交换机的 Port ID。

2.5.3 认定 LAN 的指定交换机

开始时，所有交换机都认为自己是 LAN 的指定交换机。当交换机接收到具有更低根路径花费的(同一个 LAN 中)其他交换机发来的 BPDU 时，该交换机就不再宣称自己是指定交换机。如果在一个 LAN 中有两台或多台交换机具有同样的根路径花费，具有最高优先级的交换机先为指定交换机。在一个 LAN 中，只有指定交换机可以接收和转发帧，其他交换机的所有端口都被置为阻塞状态。

如果指定交换机在某个时刻收到了 LAN 上其他交换机因竞争指定交换机而发来的配置 BPDU，该指定交换机将发送一个回应的配置 BPDU，以重新确定指定交换机。

1. 决定指定端口

在 LAN 的指定交换机中，与该 LAN 相连的端口为指定端口。若指定交换机有两个或多个端口与该 LAN 相连，那么具有最低标识的端口为指定端口。

除了根端口和指定端口外，其他端口都将置为阻塞状态。这样，在决定了根交换机、交换机的根端口以及每个 LAN 的指定交换机和指定端口后，一个生成树的拓扑结构就产生了。

2. STP 生成树形成方法

① 网络中选择一台交换机为根交换机(Root Bridge)；

② 除根交换机外的每台交换机都有一个根口(Root Port)，提供最短路径到根交换机的端口；

③ 每台交换机都计算出到根交换机的最短路径；

④ 每个 LAN 都有指定交换机(Designated Bridge)，位于该 LAN 与根交换机之间的最短路径中。指定交换机和 LAN 相连的端口称为指定端口(Designated Port)；

⑤ 根口和指定端口进入转发(Forwarding)状态；

⑥ 其他冗余端口处于阻塞(Blocking 或 Discarding)状态。

2.5.4　拓扑变化

拓扑信息在网络上的传播有一个时间限制，该时间信息包含在每个配置 BPDU 中，即消息时限。每台交换机存储来自 LAN 指定端口的协议信息，并监视这些信息存储的时间。在正常稳定状态下，根交换机定期发送配置消息以保证拓扑信息不超时。如果根交换机失效，其他交换机中的协议信息就会超时，新的拓扑结构很快在网络中传播。

当某台交换机检测到拓扑变化时，它向根交换机方向的指定交换机以拓扑变化通知定时器的时间间隔定期发送拓扑变化通知 BPDU，直到收到指定交换机发来的确认拓扑变化信息(这个确认信号在配置 BPDU 中，即拓扑变化标志位置位)。指定交换机重复以上过程，继续向根交换机方向的交换机发送拓扑变化通知 BPDU。这样，拓扑变化的通知最终传到根交换机。根交换机收到这个通知，或其自身改变了拓扑结构，将发送一段时间的配置 BPDU。在配置 BPDU 中，拓扑变化标志位被置位。所有交换机将会收到一条或多条配置消息，并使用转发延时参数的值来更新过滤数据库中的地址。所有交换机将重新决定根交换机、交换机的根端口以及每个 LAN 的指定交换机和指定端口，生成树的拓扑结构也就重新决定了。

2.5.5　STP 的端口状态

运行生成树协议的交换机上的端口总是处于下面四个状态中的一个：

① 阻塞：所有端口以阻塞状态启动，以防止回路。由生成树确定哪个端口切换为转

发状态，处于阻塞状态的端口不转发数据帧，但可接收 BPDU。

② 监听：不转发数据帧，但检测 BPDU（临时状态）。

③ 学习：不转发数据帧，但学习 MAC 地址表（临时状态）。

④ 转发：可以传送和接收数据帧。

在正常操作期间，端口处于转发或阻塞状态。当检测到网络拓扑结构有变化时，交换机会自动进行状态转换。在此期间，端口暂时处于监听和学习状态。

生成树经过一段时间（默认值是 50s）稳定之后，所有端口要么进入转发状态，要么进入阻塞状态。STP BPDU 仍然会定时从各个网桥的指定端口发出，以维护链路的状态。如果网络拓扑发生变化，生成树将重新计算，端口状态随之改变。

当拓扑发生变化时，新的配置消息要经过一定的延时才能传播到整个网络，这个延时称为 Forward Delay，协议默认值是 15s。在所有网桥收到这个变化的消息之前，若旧拓扑结构中处于转发的端口还没有发现自己应该在新的拓扑中停止转发，则可能存在临时环路。为了解决临时环路的问题，生成树使用了一种定时器策略，即在端口从阻塞状态到转发状态中间加上一个只学习 MAC 地址但不参与转发的中间状态，两次状态切换的时间长度都是 Forward Delay，以保证在拓扑变化的时候不会产生临时环路。但是，这个看似良好的解决方案实际上带来的是至少两倍 Forward Delay 的收敛时间。

在默认情况下，交换机端口由阻塞状态到侦听状态的转发时间为 20s。

2.5.6 快速生成树协议

为了解决 STP 协议收敛时间长这个缺陷，在 21 世纪初 IEEE 推出了 802.1w 标准，作为对 802.1d 标准的补充。在 IEEE 802.1w 标准里定义了快速生成树协议（RSTP，Rapid Spanning Tree Protocol）。RSTP 协议在 STP 协议基础上做了三点重要改进，使得收敛速度快得多（最快 1s 以内）。

第一点改进：为根端口和指定端口设置了快速切换用的替换端口（Alternate Port）和备份端口（Backup Port）。在根端口/指定端口失效的情况下，替换端口/备份端口会无延时地进入转发状态。在图 2-21 中，所有网桥都运行 RSTP 协议，SW1 是根桥。假设 SW2 的端口 1 是根端口，端口 2 将能够识别这种拓扑结构，成为根端口的替换端口，进入阻塞状态。在端口 1 所在链路失效的情况下，端口 2 能够立即进入转发状态，无须等待两倍 Forward Delay 时间。

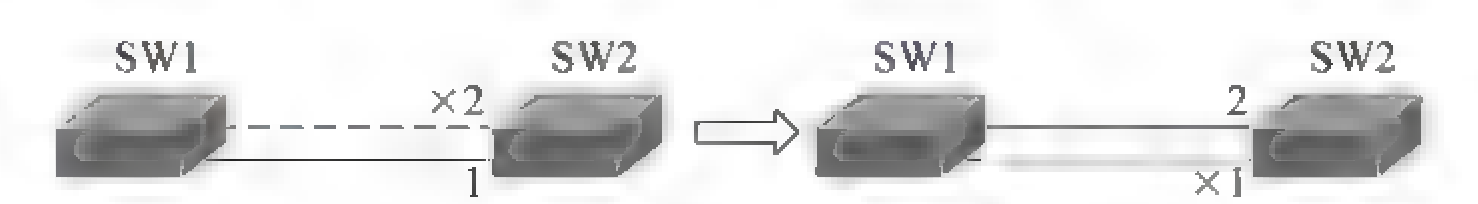


图 2-21 RSTP 冗余链路快速切换示意图

第二点改进：在只连接了两个交换端口的点对点链路中，指定端口只需与下游网桥进行一次握手就可以无延时地进入转发状态。如果是连接了三个以上网桥的共享链路，

下游网桥不会响应上游指定端口发出的握手请求，只能等待两倍 Forward Delay 时间进入转发状态。

第三点改进：直接与终端相连，而不是把其他网桥相连的端口定义为边缘端口（Edge Port）。边缘端口可以直接进入转发状态，没有任何延时。由于网桥无法知道端口是否直接与终端相连，所以需要手动配置。

可见，RSTP 协议相对于 STP 协议的确改进了很多。为了支持这些改进，BPDU 的格式做了一些修改。RSTP 协议向下兼容 STP 协议，可以混合组网。虽然如此，RSTP 和 STP 同属单生成树 SST（Single Spanning Tree），有很多缺陷，主要表现在下面三个方面：

第一点缺陷：由于整个交换网络只有一棵生成树，在网络规模比较大的时候会导致较长的收敛时间，拓扑改变的影响面也较大。

第二点缺陷：近些年 IEEE 802.1q 大行其道，逐渐成为交换机的标准协议。在网络结构对称的情况下，单生成树没什么大碍。但在网络结构不对称的时候，单生成树会影响网络的连通性。

如图 2-22 所示，假设 SW1 是根桥，实线链路是 VLAN 10，虚线链路是 802.1q 的 Trunk 链路，聚合了 VLAN 10 和 VLAN 20。当 SW2 的 Trunk 口被阻塞的时候，SW1 和 SW2 之间 VLAN 20 的通路就被切断了。

第三点缺陷：链路被阻塞后将不承载任何流量，造成了带宽的极大浪费，这在环形城域网的情况下比较明显。

如图 2-23 所示，假设 SW1 是根桥，SW4 的一个端口被阻塞。在这种情况下，SW2 和 SW4 之间铺设的光纤将不承载任何流量，所有 SW2 和 SW4 之间的业务流量都将经过 SW1 和 SW3 转发，增加了其他几条链路的负担。

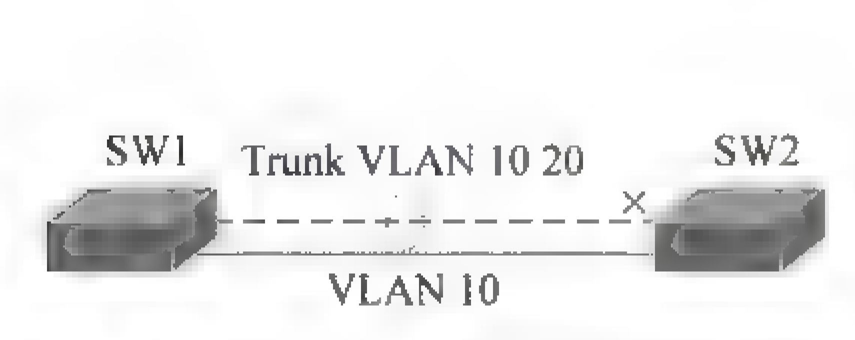


图 2-22　非对称网络示意图

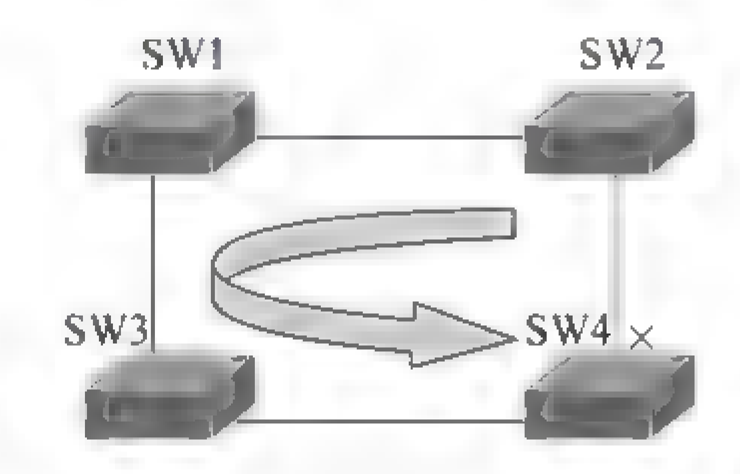


图 2-23　SST 带宽利用率低下示意图

2.5.7　配置 STP 和 RSTP 协议

1. 生成树的默认配置

关闭 STP，且 STP Priority 是 32768，STP Port Priority 是 128。STP Port Cost 根据端口速率自动判断；Hello Time 设为 2s；Forward delay Time 设为 15s；Max age Time 设为 20s。

2. 打开、关闭生成树协议

可通过 spanning-tree reset 命令让生成树参数恢复到默认配置。

```
Switch(config)#Spanning-tree
```

如果要关闭生成树协议，用 no spanning-tree 全局配置命令进行设置。

3. 配置生成树的类型

```
Switch(config)#
Spanning-tree mode STP/RSTP
```

4. 配置交换机优先级

```
Switch(config)#spanning-tree priority <0-61440>
                                   !("0"或 4096 的倍数,共 16 个,默认值为 32768)
```

如果要恢复到默认值，用 no spanning-tree priority 全局配置命令进行设置。

5. 配置交换机端口优先级

```
Switch(config-if)#spanning-tree port-priority <0-240>
                                   !(0 或 16 的倍数,共 16 个,默认值为 128)
```

如果要恢复到默认值，用 no spanning-tree port-priority 接口配置命令进行设置。

6. STP 和 RSTP 信息显示

```
SwitchA#show spanning-tree                              !显示交换机生成树的状态
SwitchA#show spanning-tree interface fastthernet 0/1    !显示交换机接口
```

规律总结(检查)

随着 Internet 的高速发展，人们对通信的需求逐渐从传统的电话、传真、电报等低速业务向高速 Internet 接入、可视电话、视频点播等宽带业务领域延伸，用户对上网速率的要求也越来越高。在这种条件下，以太网接入因其成本低、速度高、使用简单而备受市场的关注。交换机设备作为局域网中的一种很重要的“枢纽”设备，其工作状态的好坏直接决定着整个局域网的运行稳定性。

交换(switching)是按照通信两端传输信息的需要，用人工或设备自动完成的方法，把要传输的信息送到符合要求的相应路由上的技术统称。广义的交换机(switch)就是一种在通信系统中完成信息交换功能的设备。

在当今社会，网络技术发展迅猛，以太网占据了统治地位。为了适应网络应用深化带来的挑战，网络的规模和速度都在急剧发展，局域网的速度从最初的 10Mbps 提高到 100Mbps，千兆以太网技术已得到普遍应用。

对于用户来说，在降低成本的前提下，保证网络的高可靠性、高性能、易维护、易扩展，

与采用何种组网技术密切相关；对于设备厂商来说，在保证实现用户网络功能的基础上，为取得更可观的利润，要选择采用性能优异的组网技术。

交换机拥有一条很高带宽的背部总线和内部交换矩阵，交换机的所有端口都挂接在这条背部总线上。控制电路收到数据包以后，处理端口会查找内存中的地址对照表，以确定目的 MAC(网卡的硬件地址)的 NIC(网卡)挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口。目的 MAC 若不存在，将数据包广播到所有的端口，接收端口回应后，交换机会“学习”新的地址，并把它添加到内部 MAC 地址表中。

使用交换机可以把网络“分段”。通过对照 MAC 地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效地隔离广播风暴，减少误包和错包的出现，避免共享冲突。

交换机在同一时刻可进行多个端口对之间的数据传输。每一个端口都可视为独立的网段，连接在其上的网络设备独自享有全部带宽，无须同其他设备竞争使用。当节点 A 向节点 D 发送数据时，节点 B 可同时向节点 C 发送数据，而且这两个传输都享有网络的全部带宽，都有自己的虚拟连接。假使这里使用的是 10Mbps 以太网交换机，该交换机的总流通量为 2×10Mbps=20Mbps，而使用 10Mbps 共享式 HUB，一个 HUB 的总流通量不会超出 10Mbps。

总之，交换机是一种基于 MAC 地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC 地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。因此，要根据实际的网络构建情况来选择交换机，通过配置交换设备实现对网络的管理。

拓展提高(拓展)

1. VTP

(1) VTP 简介

VTP(VLAN Trunking Protocol)是 VLAN 中继协议，也称为虚拟局域网干道协议。

VTP 是 OSI 参考模型第二层的通信协议，主要用于管理在同一个域的网络范围内 VLAN 的建立、删除和重命名。在一台 VTP Server 上配置一个新的 VLAN 时，该 VLAN 的配置信息将自动传播到本域内的其他所有交换机。这些交换机会自动地接收配置信息，使其 VLAN 的配置与 VTP Server 保持一致，从而减少在多台设备上配置同一个 VLAN 信息的工作量，而且保持了 VLAN 配置的统一性。

VTP 通过网络(ISL 帧或 Cisco 私有 DTP 帧)保持 VLAN 配置统一性。如果在 VTP 服务器上增加、删除、调整了 VLAN，会自动地将信息向网络中的其他交换机广播。此外，VTP 减小了那些可能导致安全问题的配置。有了 VTP，就可以在一台交换机上集中进行配置变更，所做的变更会被自动传播到网络中所有其他的交换机上。

VTP 有三种工作模式，即 VTP Server，VTP Client 和 VTP Transparent。一般情况下，一个 VTP 域内的网络只设一个 VTP Server。VTP Server 维护该 VTP 域中的所有 VLAN 信息列表，VTP Server 可以建立、删除或修改 VLAN。VTP Client 虽然也维护所

有 VLAN 信息列表，但其 VLAN 配置信息是从 VTP Server 学到的，VTP Client 不能建立、删除或修改 VLAN。VTP Transparent 相当于一台独立的交换机，它不参与 VTP 工作，不从 VTP Server 学习 VLAN 的配置信息，而只拥有本设备上自己维护的 VLAN 信息。VTP Transparent 可以建立、删除和修改本机上的 VLAN 信息。

当交换机工作在 VTP Server 或 VTP Transparent 模式时，能在交换机配置 VLAN。可以使用 CLI、控制台菜单、MIB(当使用简单网络管理协议管理工作站时)修改 VLAN 配置。

例如，增加了一个 VLAN，VTP 将广播这个新的 VLAN，Server 和 Client 的 Trunk 口准备接收信息。

在交换机自动转到 VTP 的 Client 模式后，它会传送广播信息并从广播中学习新的信息。但是，不能通过 MIB，CLI 或者控制台来增加、删除、修改 VLAN。VTP Client 端不能在非易失存储器中保存 VLAN 信息。当启动时，它会通过 Trunk 口接收广播信息，学习配置信息。

(2) 传送 VTP 信息

每台交换机用 VTP 广播 Trunk 口的管理域，定义特定的 VLAN 边界、其配置修订号、已知 VLAN 和特定参数。在一个 VTP 管理域登记后，交换机才能工作。

通过 Trunk 口，VTP Server 向其他交换机传输信息和接收更新。VTP Server 也在 NVRAM 中保存本 VTP 管理域信息中 VLAN 的列表。VTP 能通过统一的名字和内部列表动态显示管理域中的 VLAN。

VTP 信息在全部干线连接上传输，包括 ISL，IEEE 802.10 和 LANE。VTP MIB 为 VTP 提供 SNMP 工具，并允许浏览 VTP 参数配置。

VTP 建立共用的配置值和发布下列共用的配置信息：

① VLAN ID(ISL)

② 仿效 LAN 的名字(ATM LANE)

③ IEEE 802.10 SAID 值(FDDI)

④ VLAN 中最大的传输单元(MTU)大小

⑤ 帧格式

VTP 协议是 Cisco 公司的专用协议，大多数 Catalys 交换机都支持该协议。VTP 可以减少 VLAN 的相关管理任务。

在 VTP 域中有以下两个重要的概念：

① VTP 域：也称 VLAN 管理域，由一台以上共享 VTP 域名的相互连接的交换机组成。也就是说，VTP 域是一组域名相同并通过中继链路相互连接的交换机。

② VTP 通告：在交换机之间用来传递 VLAN 信息的数据包称为 VTP 数据包。

2. PVST/PVST+

“每个 VLAN 都生成一棵树”是一种比较直接而且最简单的解决方法，它能够保证每一个 VLAN 都不存在环路。但是由于种种原因，以这种方式工作的生成树协议并没有形成标准，而是各厂商各有一套，尤其以 Cisco 公司的 VLAN 生成树 PVST(Per VLAN

Spanning Tree)为代表。

为了携带更多的信息，PVST BPDU 的格式和 STP/RSTP BPDU 格式不同，发送的目的地址改成了 Cisco 保留地址 01 00 0C CC CC CD，而且在 VLAN Trunk 的情况下，PVST BPDU 被贴上了 802.1q VLAN 标签。所以，PVST 协议不兼容 STP/RSTP 协议。

Cisco 公司很快又推出了经过改进的 PVST+协议，并成为交换机产品的默认生成树协议。经过改进的 PVST+协议在 VLAN 1 上运行的是普通 STP 协议，在其他 VLAN 上运行 PVST 协议。PVST+协议可以与 STP/RSTP 互通，在 VLAN 1 上的生成树状态按照 STP 协议计算。在其他 VLAN 上，普通交换机只会把 PVST BPDU 当作多播报文按照 VLAN 号进行转发。这并不影响环路的消除，只是 VLAN 1 和其他 VLAN 的根桥状态可能不一致。

如图 2-24 所示，所有链路默认 VLAN 是 VLAN 1，并且都聚合了 VLAN 10 和 VLAN 20。SW1 和 SW3 运行单生成树 SST 协议，而 SW2 运行 PVST+协议。在 VLAN 1 上，可能 SW1 是根桥，SW2 的端口 1 被阻塞。在 VLAN 10 和 VLAN 20 上，SW2 只能看到自己的 PVST BPDU，所以在这两个 VLAN 上，它认为自己是根桥。VLAN 10 和 VLAN 20 的 PVST BPDU 会被 SW1 和 SW3 转发，所以 SW2 检测到这种环路后，会在端口 2 上阻塞 VLAN 10 和 VLAN 20。这就是 PVST+协议提供的 STP/RSTP 兼容性。可以看出，网络中的二层环路能够被识别并消除，强制根桥的一致性是没有任何意义的。

由于每个 VLAN 都有一棵独立的生成树，单生成树的种种缺陷都被克服了。同时，PVST 具有另一个优点，那就是二层负载均衡。

如图 2-25 所示，四台设备都运行 PVST+协议，并且都 Trunk 了 VLAN 10 和 VLAN 20。假设 SW1 是所有 VLAN 的根桥，通过配置可以使得 SW4 端口 1 上的 VLAN 10 和端口 2 上的 VLAN 20 阻塞，SW4 端口 1 所在的链路仍然可以承载 VLAN 20 的流量，端口 2 所在的链路也可以承载 VLAN 10 的流量，同时具备链路备份的功能。这在以往的单生成树情况下是无法实现的。

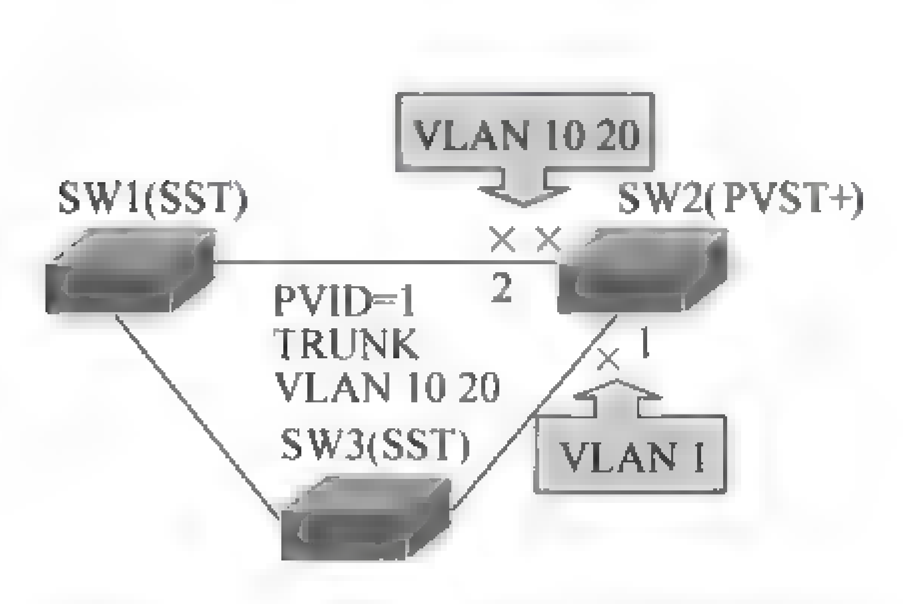


图 2-24 PVST+与 SST 对接示意图

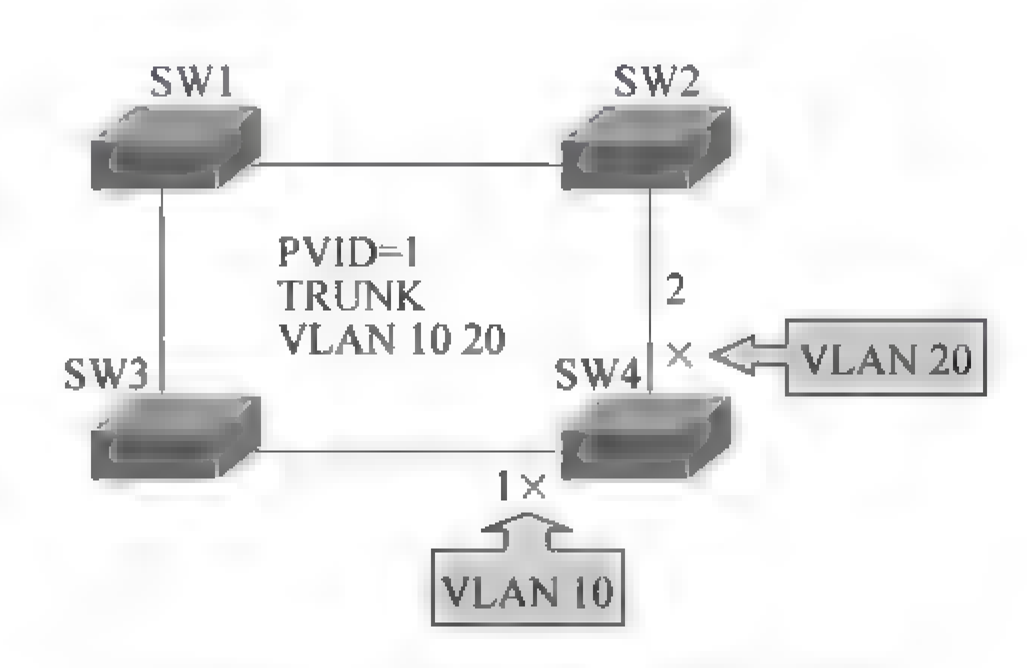


图 2-25 PVST+负载均衡示意图

PVST/PVST+协议实现了 VLAN 认知能力和负载均衡能力，但是新技术带来了新问题，PVST/PVST+协议也有其缺陷。

第一，由于每个 VLAN 都需要生成一棵树，PVST BPDU 的通信量将正比于 Trunk 的 VLAN 个数。

第二，在 VLAN 个数比较多的时候，维护多棵生成树的计算量和资源占用量将急剧增长。特别是当 Trunk 了很多 VLAN 的接口状态变化的时候，所有生成树的状态都要重新计算，CPU 将不堪重负。所以，Cisco 交换机限制了 VLAN 的使用个数，不建议在一个端口上 Trunk 很多 VLAN。

第三，由于协议的私有性，PVST/PVST＋不能像 STP/RSTP 一样得到广泛的支持，不同厂家的设备并不能在这种模式下直接互通，只能通过一些变通的方式实现。

一般情况下，网络的拓扑结构不会频繁变化，所以 PVST/PVST＋的这些缺点并不致命。但是，Trunk 口的大量 VLAN 需求还是存在的。于是，Cisco 公司对 PVST/PVST＋又做了进一步改进，推出了多实例化的 MISTP 协议。

3. MISTP/MSTP

多实例生成树协议（MISTP，Multi-Instance Spanning Tree Protocol）定义了“实例”（Instance）的概念。简单地说，STP/RSTP 是基于端口的，PVST/PVST＋是基于 VLAN 的，MISTP 是基于实例的。所谓实例，就是多个 VLAN 的一个集合，通过将多个 VLAN 捆绑到一个实例中的方法可以节省通信开销和资源占用率。

在使用 MISTP 的时候，可以把多个相同拓扑结构的 VLAN 映射到一个实例里，这些 VLAN 在端口上的转发状态将取决于对应实例在 MISTP 里的状态。值得注意的是，网络里的所有交换机的 VLAN 和实例映射关系必须都一致，否则会影响网络连通性。为了检测这种错误，MISTP BPDU 里除了携带实例号以外，还要携带实例对应的 VLAN 关系等信息。MISTP 协议不处理 STP/RSTP/PVST BPDU，所以不能兼容 STP/RSTP 协议，甚至不能向下兼容 PVST/PVST＋协议，在一起组网的时候会出现环路。为了让网络平滑地从 PVST＋模式迁移到 MISTP 模式，Cisco 公司在交换机产品里做了一个处理 PVST BPDU 的混合模式 MISTP-PVST＋。网络升级的时候，需要先把设备都设置成 MISTP-PVST＋模式，再全部设置成 MISTP 模式。

MISTP 的优点是显而易见的。它既有 PVST 的 VLAN 认知能力和负载均衡能力，又拥有可以和 SST 相媲美的低 CPU 占用率。不过，极差的向下兼容性和协议的私有性阻挡了 MISTP 的大范围应用。

MISTP 协议精妙的地方在于把支持 MISTP 的交换机和不支持 MISTP 的交换机划分成不同的区域，分别称做 MST 域和 SST 域。在 MST 域内部运行多实例化的生成树，在 MST 域的边缘运行 RSTP 兼容的内部生成树 IST（Internal Spanning Tree）。

如图 2-26 所示，MST 域内的交换机间使用 MISTP BPDU 交换拓扑信息，SST 域内的交换机使用 STP/RSTP/PVST＋BPDU 交换拓扑信息。在 MST 域与 SST 域之间的边缘上，SST 设备认为对接的设备也是一台 RSTP 设备。而 MST 设备在边缘端口上的状态将取决于内部生成树的状态，也就是说，端口上所有 VLAN 的生成树状态将保持一致。

MISTP 设备内部需要维护的生成树包括若干个内部生成树 IST，其个数和连接了多少个 SST 域有关。另外，还有若干个多生成树实例 MSTI（Multiple Spanning Tree Instance）确定的 MISTP 生成树，其个数由配置了多少个实例决定。

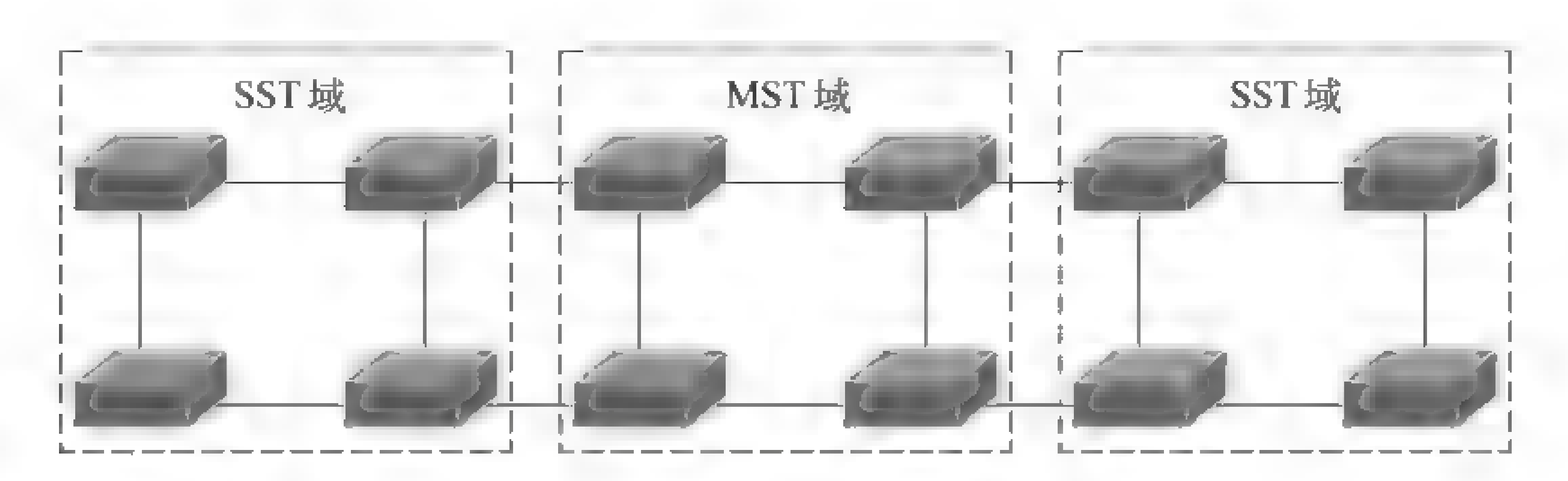


图 2-26　MISTP 工作原理示意图

MISTP 相对于之前的种种生成树协议而言，优势非常明显。MISTP 具有 VLAN 认知能力，可以实现负载均衡，可以实现类似 RSTP 的端口状态快速切换，可以捆绑多个 VLAN 到一个实例中以降低资源占用率。最难能可贵的是，MISTP 可以很好地向下兼容 STP/RSTP 协议。而且，MISTP 是 IEEE 标准协议，推广的阻力相对小得多。

可见，各项全能的 MISTP 协议能够成为当今生成树发展的一致方向。

思考训练(评估)

1. 思考与提高

(1) 简述 VLAN 的优点。
(2) VLAN 对局域网广播有什么影响?
(3) VLAN 有哪几种主要的实现方式?
(4) VLAN 帧标记的目的是什么?
(5) 比较 Port VLAN 和 Tag VLAN 的优缺点及使用场合。
(6) 简述冗余链路的产生原因。
(7) STP 协议的原理是什么?

2. 实训

(1) 观察交换机的启动过程，了解交换机的软、硬件配置；掌握交换机的命令模式，熟悉进入各个模式的基本命令。案例：某机房有 100 台计算机，现需要联网。要求：

① 画出拓扑图；
② 规划 IP 地址；
③ 推荐几种交换机，了解其软、硬件配置。

(2) 熟悉根据 Port 来划分 VLAN 的配置，了解 VLAN 如何跨交换机实现，并能利用 Trunk 端口和上层设备相连。

(3) 在一台支持 STP 协议的交换机上，通过超级终端来配置简单 STP 协议。

学习情境 3　局域网间互联

任务情境(资讯)

ThreeFour Software 软件公司发展越来越快，为了配合市场销售，公司在最近的大城市中心租用了办公室成立分支机构。现在的任务是要将总部的局域网络和分支机构的网络连接起来。为此，需要新的设备——路由器。李四购买了两台路由器，但如何选择广域网线路呢？通过了解，李四租用了电信运营商的 E1 专线作为广域网线路，采用的链路协议为 PPP。由于网络组成比较简单，李四决定使用静态路由完成连接。

在利用静态路由连接总部和分支机构之后，网络运行正常。但是静态路由在实际应用中逐渐显示出劣势。特别是在引入备份线路后，随着网络复杂程度的提高，"静态"的路由无法反映网络的实时变化情况，经常需要手动修改。大大增加了工作量，所以李四决定采用动态路由来解决这一问题。

在完成了总部和分支机构网络互联之后，公司网络有进一步访问 Internet 的需求。为此，李四在总部申请了另外一条专线用于访问 Internet。由于公司内部网络用的都是私有 IP 地址，需要通过 NAT 地址转换，将私有 IP 地址转换为 Internet 上的公有 IP 地址。

任务分析(决策)

在上述情境中，我们遇到的问题是当网络不断扩展，网络连接的范围不断扩大，这时需要租用电信运营商提供的设备和线路。在这种模式下组成的网络称为广域网。广域网可以承载不同类型的信息，如语音、视频和数据。当用户通过广域网建立连接时，或者说数据在广域网中传输时，可以选择不同的方式，由广域网的协议和网络类型决定。在广域网上实现数据传输涉及路由以及内部地址转换的问题。为此，需要了解以下内容。

1. 路由

所谓路由，就是指通过相互连接的网络把信息从源地点移动到目标地点的活动。一般来说，在路由过程中，信息会经过一个或多个中间节点。通常，人们会把路由和交换进行对比，这主要是因为在普通用户看来，两者所实现的功能是完全一样的。其实，路由和交换之间的主要区别是交换发生在 OSI 参考模型的第二层(数据链路层)，而路由发生在第三层，即网络层。这决定了路由和交换在移动信息的过程中需要使用不同的控制信息，所以两者实现各自功能的方式是不同的。

早在 40 多年前就出现了对路由技术的讨论，但是直到 20 世纪 80 年代，路由技术才逐渐进入商业化的应用。路由技术之所以在问世之初没有被广泛使用，主要是因为 80 年代之前的网络结构非常简单，路由技术没有用武之地。直到最近十几年，大规模的互联网逐渐流行起来，为路由技术的发展提供了良好的基础和平台。

2. 路由协议

路由协议就是根据特定的判断标准和算法，计算出网络中到不同子网的最佳路径的协议。

目前主流的单播路由协议有 RIP v1/v2、OSPF v2 和 BGP v4，这些路由协议在 IOS 软件中都能提供完善的支持。

3. 路由器

路由器是一个工作在 TCP/IP 第三层，即网络层的网络设备，它的主要作用是为收到的报文寻找正确的路径，并把它们转发出去。通俗地讲，路由器就是从一个网络向另一个网络传递数据包，相当于现实生活中的邮局，用户将信件交给本地邮局，本地邮局将信件通过各种运输工具送到目的邮局，最后由目的邮局送交给收信人。

路由器是用来连接异种网络的重要网络设备，它必须具备以下性能：

① 两个或两个以上的接口(用于连接不同的网络，需要支持丰富的广域网接口)

② 协议至少实现到网络层

③ 至少支持两种以上的网络链路协议(异种网)

④ 具有存储、转发、寻径的功能

4. 路由表

路由表是保存在路由器存储器中的数据文件，其中存储了与直连网络以及远程网络相关的信息。路由表包含网络与下一跳的关联信息，如图 3-1 所示。这些关联告知路由器：要以最佳方式到达某一目的地，可以将数据包发送到特定路由器(即在到达最终目的地的途中的“下一跳”)。下一跳也可以关联到通向最终目的地的外发或送出接口。



图 3-1 路由表信息

路由器的主要工作就是为经过路由器的每个数据包寻找一条最佳传输路径，并将该数据有效地传送到目的站点。由此可见，选择最佳路径的策略即路由算法是路由器的关键所在。为了完成这项工作，在路由器中保存着各种传输路径的相关数据——路由表(Routing Table)，供路由选择时使用，表中包含的信息决定了数据转发的策略。打个比方，路由表就像我们平时使用的地图一样，标识着各种路线，路由表中保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路由表可以是由系统管理员固定设置好的，也可以由系统动态修改；可以由路由器自动调整，也可以由主机控制，主要可分为静态路由表和动态路由表两种类型。

(1) 静态路由表

由网络系统管理员事先设置好的固定的路由表称为静态(Static)路由表，一般是在系统安装时就根据网络的配置情况设定的，它不会随未来网络结构的改变而改变。

(2) 动态路由表

动态(Dynamic)路由表是路由器根据网络系统的运行情况而自动调整的路由表。路由器根据路由选择协议(Routing Protocol)提供的功能，自动学习和记忆网络运行情况，在需要时自动计算数据传输的最佳路径。

路由器在转发数据包时，要先在路由表中查找相应的路由，才能知道数据应该从哪个接口转发出去。那么，路由器是如何建立路由表的呢？一般有以下三种途径：

① 直连网络：路由器自动添加和自己直接连接的网络路由；

② 静态路由：管理员手动输入到路由器的路由；

③ 动态路由：由路由协议动态建立的路由。

5. 路由器的基本工作过程

路由器在网络中所起的作用就是数据转发。当路由器的一个接口收到数据包之后，根据数据包的目的地址信息，按照路由表中存储的路由信息将数据包从另一个接口转发，这就是一个简单的路由过程。

路由的基本工作过程可以按照IP协议工作的情况来描述，网络结构如图3-2所示。路由器R1的两个接口分别连接到网络172.16.1.0和172.16.2.0上。当PC1要发送一个数据包到PC2时，在路由器R1的Fa0接口收到数据包后，通过计算查询路由表，可以发现PC2的地址与路由器R1的Fa1接口相连，路由器就将数据包通过接口Fa1转发给PC2，一个路由过程就完成了。

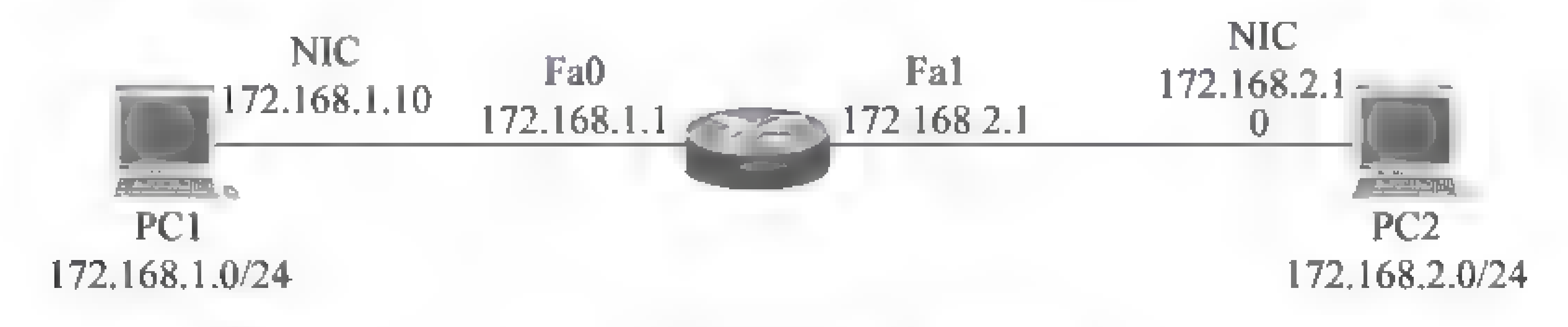


图3-2 基本的路由器连接

6. 路由器的基本协议与技术

路由协议是路由器软件中重要的组成部分。路由器的路由功能就是通过这些路由协议

来实现的，路由协议是用来建立以及维护路由表。路由表记录转发数据到已知目的节点的最佳路径，有了它，只需直接按路径转发数据包即可，大大提高了数据转发的速度和效率。

(1) 路由协议的种类

除了按路由是否变化分为静态路由和动态路由外，在路由协议中还根据是否在一个自治域内部使用，将动态路由协议分为内部网关协议(IGP)和外部网关协议(EGP)。这里的自治域指一个具有统一管理机构、统一路由策略的网络。自治域内部采用的路由选择协议称为内部网关协议，常用的有 RIP 和 OSPF；外部网关协议主要用于多个自治域之间的路由选择，常用的是 BGP 和 BGP-4，下面分别介绍。

① RIP 协议

RIP 是推出时间最长的路由协议，也是最简单的路由协议。它主要通过传递路由信息(路由表)来广播路由，每隔 30s 广播一次路由表，维护相邻路由器的关系，同时根据收到的路由表计算自己的路由表。RIP 运行简单，适用于小型网络，互联网上还在部分使用着 RIP。

② OSPF 协议

OSPF 协议是"开放式最短路径优先"的缩写。"开放"是针对当时某些厂家的"私有"路由协议而言的，正是因为协议的开放性，才使得 OSPF 具有强大的生命力和广泛的用途。它通过传递链路状态(连接信息)来得到网络信息，维护一张网络有向拓扑图，利用最小生成树算法得到路由表。OSPF 是一种相对复杂的路由协议。

总的来说，OSPF 和 RIP 都是自治系统内部的路由协议，适合于单一的 ISP(自治系统)使用。一般来说，整个互联网并不适合运行单一的路由协议，因为各 ISP 有自己的利益，不愿意提供自身网络详细的路由信息。为了保证各 ISP 的利益，标准化组织制定了 ISP 间的路由协议 BGP。

③ BGP 协议

BGP 处理各 ISP 之间的路由传递，其特点是有丰富的路由策略，这是 RIP 和 OSPF 协议无法做到的，因为它们需要全局的信息计算路由表。BGP 通过 ISP 边界的路由器加上一定的策略，选择过滤路由，把 RIP、OSPF 和 BGP 的路由发送到对方。全局范围的、广泛的互联网是 BGP 处理多个 ISP 间路由的实例。BGP 的出现引起了互联网的重大变革，它把多个 ISP 有机地连接起来，真正形成全球范围的网络，带来的副作用是互联网的"路由爆炸"，现在互联网的路由大概是 60000 条，这还是经过"聚合"后的数字。配置 BGP 需要对用户需求、网络现状和 BGP 协议非常了解，还需要非常小心，BGP 运行在相对核心的地位，一旦出错，造成的损失可能会很大。

(2) 路由器主要技术

① VPN 技术

VPN(Virtual Private Network，虚拟专用网络)解决方案是路由器的重要技术之一。路由器的 VPN 解决方案主要采用访问控制、数据加密、NAT(Network Address Translation，网络地址转换协议)等几种方案。

② QoS 技术

QoS(Quality of Service，服务质量)本来是 ATM(Asynchronous Transmit Mode，异

步传输模式)中的专用术语,在 IP 上原来是不谈 QoS 的,但利用 IP 传输 VOD 等多媒体信息的应用越来越多,IP 作为一个打包协议显得力不从心:延时长且不为定值,丢包造成信号不连续且失真大。为解决这些问题,各厂商提供了若干解决方案:第一种方案基于不同对象的优先级,某些设备(多为多媒体应用)发送的数据包可以后到先传。第二种方案基于协议的优先级,用户可定义哪种协议的优先级高,可后到先传,Intel 公司和 Cisco 公司都支持;第三种方案是做链路聚合(MLPPP,Multi Link Point to Point Protocol),Cisco 公司支持将连接两点的多条线路做带宽汇聚,从而提高带宽;第四种方案是做资源预留(RSVP,Resource Reservation Protocol),它将一部分带宽固定地分给多媒体信号,其他协议无论如何拥挤,也不得占用这部分带宽。这几种解决方案都能有效地提高传输质量。

(3) IPv6 技术

迅速发展的互联网不再是仅仅连接计算机的网络,它将发展成与电话网、有线电视网类似的信息通信基础设施。因此,正在使用的 IP(互联网协议)难以胜任,人们迫切希望下一代 IP 即 IPv6 的出现。

IPv6 是 IP 的一种版本,在互联网通信协议 TCP/IP 中是 OSI 模型第三层(网络层)的传输协议。它同目前广泛使用的、1974 年便提出的 IPv4 相比,地址由 32 位扩充到 128 位。从理论上说,地址的数量由原先的 4.3×109 个增加到 4.3×1038 个。

7. 广域网链路层协议

在地域分布很广、很分散,以致无法用直接连接来接入局域网的场合,广域网(WAN)通过专用的或交换式的连接把计算机连接起来。这种广域连接可以是通过公众网建立的,也可以是通过服务于某个专门部门的专用网建立起来的。相对来说,广域网显得比较复杂,主要是用于广域传输的协议比较多,包括 PPP(点对点协议)、DDN(数字专线)、ISDN(综合业务数字网)、X.25、FR(帧中继)和 ATM(异步传输模式)等。

(1) PPP(点对点协议)

PPP(点对点协议)主要用于"拨号上网"这种广域连接模式。一般来说,一些无法使用专门的网络线连接的双方(比如说家庭用户、移动用户)需要广域连接的时候,可以借助分布最广的公用交换电话网来实现。当用户要浏览互联网网页的时候,首先通过调制解调器连接到电话线,然后将在远方服务器的内容通过电话线传送到用户的计算机中;或者,当用户要发送电子邮件的时候,将写好的邮件从电话线传送出去。另外,两个不同城市的两台计算机要互相传送数据,也可以通过装在两台计算机上的调制解调器,让其中一台呼叫另一台(拨打它的电话号码),建立点对点的连接来实现。迄今为止,拨号上网是绝大多数家庭用户和小型办公室用户实现广域连接的一种最常用的手段。但是因为其传输线路是模拟的,所以传输速度较慢。

用户接入 Internet,在传送数据时都需要有数据链路层协议,其中最广泛的是串行线路网际协议(SLIP)和点对点协议(PPP)。由于 SLIP 仅支持 IP,主要用于低速(不超过 19.2Kbps)的交互性业务,未成为 Internet 的标准协议。为了改进 SLIP,人们制定了点对点协议 PPP(Point to-Point Protocol)。

(2) ISDN(综合业务数字网)

ISDN 经历了一个极为漫长的"进化"过程。如果你常看一些网络界的时报，一定不会在 10 年前就对它有所耳闻。在它出现的时候，远程通信界的专家们都声称它是未来的公用电话、电信接口。但是它不够经济，严重地阻碍了其广泛应用。中国电信用了一个形象的名字"一线通"描述其特点：ISDN 将数据、声音、视频信号集成进一根数字电话线路，提供有效、经济的途径，将用户与高带宽数字服务相连。ISDN 分为 N-ISDN(窄带 ISDN)和 B-ISDN(宽带 ISDN)两种。常用于家庭及小型办公室的是 N-ISDN，它提供的基本速率接口(BRI)服务由 2 条 B 信道和 1 条 D 信道组成(2B+D)，其中 B 信道速率为 64Kbps，D 信道速率为 16Kbps。B-ISDN 提供的主要速率接口(PRI)在不同的国家不尽相同。在北美、日本为 23 条速率 64Kbps 的 B 信道和 1 条速率也为 64Kbps 的 D 信道，总速率为 1.544Mbps，即 23B+D。在欧洲、澳洲及其他国家，一般由 30 条速率 64Kbps 的 B 信道和 1 条速率也为 64Kbps 的 D 信道构成，总的接口速率可达到 2.048Mbps，也就是 30B+D。

(3) xDSL

xDSL 是 DSL (Digital Subscriber Line)的统称，即数字用户线路，是以铜电话线为传输介质的传输技术组合。DSL 技术主要分为对称和非对称两大类。

① HDSL(高速对称 DSL)：是 xDSL 技术中最成熟的，它利用两对双绞线传输，支持 $N\times64$Kbps 和多种速率，最高可达 E1 速率。

② SDSL(对称 DSL)：利用单对双绞线传输，支持多种速率，最高到 T1/E1。

③ MVL：Paradyne 公司开发的低成本对称 DSL 传输技术，可以提供上、下行 768Kbps 的传输速率，传输距离可达 6km。

④ ADSL(非对称 DSL)：利用现有铜双绞线(即普通电话线)，提高到 8Mbps 下行速度，1Mbps 上行速度，传输距离 3～5km。

(4) DDN

我国原邮电部于 1994 年 10 月完成了全国数字数据骨干网的一期建设。这是一个利用光纤、数字微波或卫星数字交驻连接设备组成的数字数据业务网。这些数字线路出租给最终用户。由于在用户使用 PPP 协议拨号上网的时候，发送、接收数据所使用的电话线路是不明确的，速率根据当时线路的拥塞情况不同而不同，所以其传输是低速且不稳定的。对于某些需要更高传输速度和质量的用户，可以租用 DDN 线路。这相当于用户与电信局端直接用一条定制带宽的专用电话线路相连，大大提高了数据传输的稳定性和速度。这项业务开通后，被用户广泛采用。在 DDN 的客户端需要一个称为 DDN Modem 的 CSU/DSU 设备以及一个路由器，其价格与 DDN 线路的带宽相关。

(5) X.25

X.25 是历史最悠久的广域数据传输协议。它是所有广域数据传输协议的鼻祖，为广域传输做出了很大的贡献，但现在其应用越来越少。

(6) FR(帧中继)

作为 X.25 网络协议的发展，帧中继是一种高性能的广域网协议。它是 X.25 的简化版本，省去了 X.25 的一些强制功能，如提供窗口技术和数据重发功能，这是因为帧中继

的设计是以网络的传输环境已经有了很大的提高为前提的。

1990 年，Cisco，Digital Equipment，Northern TeleCom 和 StartaCom 等公司组成一个联合体，共同开发了帧中继技术。此后，帧中继技术有了迅猛发展。从整个连接上，帧中继与 X.25 相当类似，但它在数据分组确认和差错校验方法上有了很大的简化，而且分组的转发有了改变。帧中继只要接到分组头，就开始转发，这进一步提高了速度。但是，需要强调的是，帧中继在网络环境不好的情况下，将无法像 X.25 那样提供较好的传输质量，而且可能会使传输质量急剧下降。

任务设计（计划）

简单了解了用于局域网互联涉及的基本概念后，下面根据 ThreeFour Software 公司的具体情况提出 5 个任务来解决问题。

任务 3.1　路由器基本配置
任务 3.2　静态路由基本配置
任务 3.3　动态路由基本配置
任务 3.4　PPP 协议基本配置
任务 3.5　NAT 地址转换基本配置

任务实施（实施）

任务 3.1　路由器基本配置

3.1.1　认识路由器

配置路由器之前，首先应了解其结构及配置内容。

1. 路由器的内部构成

路由器也是一台计算机，它的硬件与计算机的构成相类似，其内部是一块大规模集成电路板和一些插槽，还有处理器(CPU)、内存、接口及总线等。路由器是一台有特殊用途的专用计算机，专业用来做路由计算用的计算机。路由器与普通计算机不同，它没有显示器、硬盘和键盘等。

① 处理器：和其他计算机一样，运行 IOS 的路由器也包含了一个“中央处理器”(CPU)。不同系列和型号的路由器，CPU 不尽相同。路由器的处理器负责执行处理数据包所需的工作，比如维护路由和桥接所需的各种表格以及作出路由决定。路由器处理数据包的速度在很大程度上取决于处理器的类型。

② 随机存储器(RAM，Random Access Memory)：RAM 保存路由表、ARPCache、快交换 Cache、分组缓和(共享 RAM)和分组队列；RAM 还在路由器通电后为配置文件提供

运行内存；RAM 内容将在路由器断电或重启断电后丢失。

③ 非易失性存储器(NVRAM，Non Volatile RAM)：保存路由器的备份/启动(backup/start-up)配置文件；NVRAM 内容在断电或重启时被保持。

④ 闪存(Flash)：易擦写可编程 ROM，支持操作系统的映像和微码；Flash 内存能够进行软件升级，而不用更换处理芯片；Flash 内存在断电或重启时被保持；Flash 内存能够保存多版本的 IOS 软件。

⑤ 接口(Interface)：路由器的全部作用就是从一个网络向另一个网络传递数据包。路由器的接口在物理上将路由器连接到各种不同类型的网络上。最重要的路由器接口是串行口(它通常将路由器连接到广域网链路上)和 LAN 接口，如图 3-3 所示。

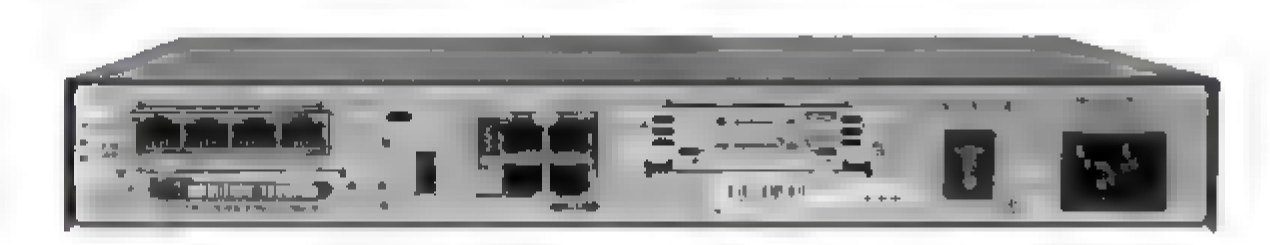


图 3-3　路由器接口

⑥ 只读存储器(ROM，Read Only Memory)：保存通电诊断、引导程序和操作系统软件；ROM 中的软件升级需要更换可插入芯片。

⑦ 操作系统软件：不同的路由器产品有不同的操作系统，如 Cisco 路由器的操作系统名称是 IOS，锐捷路由器的操作系统名称是 RGNOS，它们是一个软件映像，放在内存中。

2. 路由器的启动顺序

路由器的启动分为四部分：加电自检、加载引导(bootstrap)程序、查找并加载操作系统软件以及查找并加载配置文件。那么，路由器到底是如何加载 IOS 和配置文件的呢？下面将详细介绍。

① 加电自检(POST)是每台计算机启动时必经的一个过程。当路由器加电时，路由器 ROM 芯片上的软件执行自检。在这种自检过程中，路由器通过 ROM 执行诊断，主要针对包括 CPU、RAM 和 NVRAM 在内的几种硬件组件。自检完成后，路由器将执行引导程序。

② 自检完成后，路由器自带的引导(bootstrap)程序将从 ROM 复制到 RAM。进入 RAM 后，CPU 执行 bootstrap 程序中的指令。引导程序的主要任务是查找路由器操作系统软件，并将其加载到 RAM。此时，如果有连接到路由器的计算机，用户会看到屏幕上开始出现输出内容。如果 NVRAM 中有有效的启动命令(boot system)，则按照启动命令来启动。

③ 查找操作系统软件。路由器操作系统软件通常存储在闪存中，也可能存储在其他位置，如 TFTP(简单文件传输协议)服务器上。如果不能找到完整的操作系统软件映像，会从 ROM 将精简版的操作系统软件复制到 RAM 中。这种版本的操作系统软件一般用于帮助诊断问题，也可用于将完整版的操作系统软件加载到 RAM。如果 NVRAM 中没有有效的启动命令，则默认加载 Flash 中的第一个操作系统软件文件。

④ 查找启动配置文件。路由器操作系统软件加载后，引导程序会搜索 NVRAM

中的启动配置文件(也称为 startup-config)。此文件含有先前保存的配置命令以及参数,包括接口地址、路由信息、口令、网络管理员保存的其他配置。如果启动配置文件 startup config 位于 NVRAM,会将其复制到 RAM 作为运行配置文件 running config。如果 Flash 没有有效的操作系统软件,会试图从网络启动,查找 TFTP 服务器。

3. 路由器的 Setup 会话

当 NVRAM 里没有有效的配置文件时,路由器自动进入 Setup 会话模式;也可在命令行输入 Setup 命令进行配置。

Setup 命令是一个交互式的命令,每一个提问都有一个默认配置。如果采用默认配置,按 Enter 键即可。如果系统已经配置过,则显示目前的配置值。如果是第一次配置,则显示出厂设置。若屏幕显示" ------More ------",输入空格键继续;若要从 Setup 中退出,按 Ctrl+C 键即可。

(1) Setup 主要参数

```
主机名: hostname
特权口令:enable password
虚终端口令:virtual terminal password
路由器名字设置: Hostname string
```

(2) Setup 接口参数

设置以太网口、Token Ring 口、同步口、异步口等接口参数,包括 IP 地址、子网屏蔽、Token Ring 速率等。

(3) Setup 描述

设置参数后,系统提示是否要应用以上配置。如果回答"YES",系统将存储配置参数,系统就可以使用了。

4. Setup 相关命令

```
show config
write memory
write erase
reload
setup
```

3.1.2 初始化配置路由器

很多初学路由器的读者对路由器的初始配置可能感到很陌生,由于路由器操作系统的原因,在初始化配置时很多信息都是用英文提示的,这对初学者来说是一个很大的难题。下面以一台 Cisco 路由器的启动配置过程为例,讲解初始配置过程。

① 用 Cisco 随机带的 Console 线,一端连在 Cisco 路由器的 Console 口,一端连在计算机的 COM 口。

② 打开计算机，启动超级终端，为连接取个名字，比如 CISCO SETUP。下一步，选定连接时用 COM1 选定每秒位数为 9600，数据位为 8，奇偶校验为无，停止位为 1，数据流控制为无，最后单击“确定”按钮。

③ 打开路由器电源，超级终端将出现以下信息(以下信息中灰色字符为输入的)：

```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Self decompressing the image:
############################################################### [OK]
        Restricted Rights Legend
Use, duplication, or disclosure by the Government issubject to restrictions as set forth in
subparagraph (c) of the Commercial Computer Software - RestrictedRights clause at
FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and
ComputerSoftware clause at DFARS sec. 252.227-7013.
        cisco Systems, Inc.
        170 West Tasman Drive
        San Jose, California 95134-1706
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5) Technical
Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang
Cisco 2621 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)
        ---System Configuration Dialog---
Continue with configuration dialog? [yes/no]: y
(是否进入初始化配置对话,选 Y.对于熟悉的用户,完全可以不使用这个对话过程,直接选择 N 进
入命令行状态.)
At any point you may enter a question mark'? 'for help.Use ctrl-c to abort configuration
dialog at any prompt. Default settings are in square brackets '[]'. (在设置对话过程中的任何地
方都可以键入"?"得到系统的帮助,按 Ctrl+ C 可以退出设置过程,默认设置将显示在'[]'中.)
Basic management setup configures only enough connectivity for management of the system,
extended setup will ask you to configure each interface on the system.
Would you like to enter basic management setup? [yes/no]: n
(是否进入基本配置安装,选 N)
First, would you like to see the current interface summary? [yes]: y
(首先,是否看一下当前端口状态)
Current interface summary

Interface       IP-Address     OK? Method Status      Protocol
FastEthernet0/0 unassigned      YES manual administratively down down
FastEthernet0/1 unassigned      YES manual administratively down down
```

```
Configuring global parameters: (从此处开始,路由器设置全局参数)
Enter host name [Router]: RouterA (设备路由器名)
The enable secret is a password used to protect access to privileged EXEC and configuration modes.
This password, after entered, becomes encrypted in the configuration.
Enter enable secret: aaa (设置进入特权状态的密文)
The enable password is used when you do not specify an
enable secret password, with some older software versions, and some boot images.
Enter enable password: bbb (设置进入特权状态的密码,不能和密文相同)
The virtual terminal password is used to protect access to the router over a network
interface.
Enter virtual terminal password: ccc (设置虚拟终端访问时的密码,以备远程登录使用)
Configure SNMP Network Management? [no]: n (是否配置简单网管协议,在此选 N)
Configuring interface parameters:(配置接口参数)
Do you want to configure FastEthernet0/0 interface? [no]: y
IP address for this interface: 192.168.1.1
(配置该接口的 IP 地址为 192.168.1.1)
Subnet mask for this interface [255.255.255.0]:
配置该接口的子网掩码(默认的是 255.255.255.0,可以手工输入来修改)
Do you want to configure FastEthernet0/1 interface? [no]: y
IP address for this interface: 192.168.2.1
(配置该接口的 IP 地址为 192.168.2.1)
Subnet mask for this interface [255.255.255.0]:
(配置该接口的子网掩码(默认的是 255.255.255.0,可以手工输入来修改)
The following configuration command script was created:
!
hostname r1
enable secret 5 $1$mERr$0qc4f9z9UYCi6V2sVqpTi.
enable password bbb
line vty 0 4
password ccc
!
interface FastEthernet0/0
no shutdown
ip address 192.168.1.1 255.255.255.0
!
interface FastEthernet0/1
no shutdown
ip address 192.168.2.1 255.255.255.0
!
end
(以下提示是否保存这次设置)
[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]:
Press RETURN to get started!
(选择 2 保存设置并存入 NVRAM)
```

至此，完成了一个新路由器的基本配置，接下来可以完成更详细的配置。

任务 3.2　静态路由基本配置

3.2.1　静态路由概述

静态路由是指由网络管理员手动配置的路由信息。当网络的拓扑结构或链路状态发生变化时，网络管理员需要手动修改路由表中相关的静态路由信息。静态路由信息在默认情况下是私有的，不会传递给其他路由器。当然，网管员可以通过设置路由器，使之成为共享的。静态路由一般适用于比较简单的网络环境。在这样的环境中，网络管理员易于清楚地了解网络的拓扑结构，便于设置正确的路由信息。

还有更重要的一点就是安全。动态路由选择实际上总是力图揭示互联网络中的每一件事情。为了安全起见，隐藏网络的某些部分可能更合适些。静态路由选择就允许互联网管理人员指定在有限的网络划分中哪些部分可以公开、哪些部分应该隐藏起来。

3.2.2　静态路由的配置

通过配置静态路由，用户可以指定对某一网络访问时所要经过的路径。在网络结构比较简单，且到达某一网络所经过的路径唯一的情况下，可采用静态路由。

例如，配置如图 3-4 所示网络中路由器的静态路由（假定图中的所有网络均采用 C 类地址掩码）。

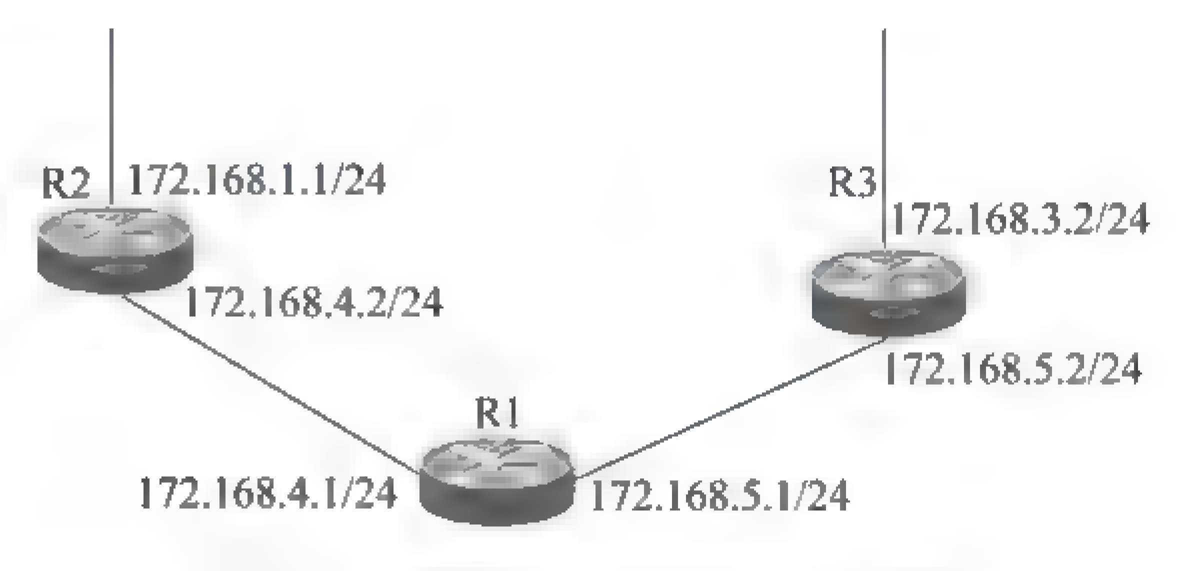


图 3-4　静态路由配置网络拓扑图

（1）路由器 R1 的配置

```
hostname R1
interface ethernet 0
ip address 172.16.4.1 255.255.255.0
interface ethernet 1
ip address 172.16.5.1 255.255.255.0
ip route 172.16.1.0 255.255.255.0 172.16.4.2
ip route 172.16.3.0 255.255.255.0 172.16.5.2
```

(2) 路由器 R2 的配置

```
hostname R2
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
interface ethernet 1
ip address 172.16.4.2 255.255.255.0
ip route 172.16.3.0 255.255.255.0 172.16.4.1
ip route 172.16.5.0 255.255.255.0 172.16.4.1
```

(3) 路由器 R3 的配置

```
hostname R3
interface ethernet 0
ip address 172.16.3.2 255.255.255.0
interface ethernet 1
ip address 172.16.5.2 255.255.255.0
ip route 172.16.1.0 255.255.255.0 172.16.5.1
ip route 172.16.4.0 255.255.255.0 172.16.5.1
```

通过以上配置,为局域网中的每台路由器都建立了静态路由。

3.2.3 默认路由的配置

在图 3-4 所示网络中,假定在局域网中要通过 R1 向外连接 Internet,路由器下一跳接口地址为 172.16.2.2,由于此时不知道从 R1 向外连接的网络的具体地址,也就无法配置静态路由,此时需要启用默认路由,把默认路由指向网络服务提供商。这样,路由器 R1 只需要知道它自己内部网络中的各个目标网络地址即可,默认路由将把去往其他地址的数据包全部转发给 Internet 服务提供商。本例默认路由的实现命令为:

```
ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

任务 3.3 动态路由基本配置

动态路由器上的路由表项是通过相互连接的路由器之间交换信息,然后按照一定的算法优化出来的,这些路由信息在一定时间间隔里更新,以适应不断变化的网络,随时获得最优的寻路效果。为了实现 IP 分组的高效寻路,IETF 制定了多种寻路协议,其中,用于自治系统(AS,Autonomous System)的内部网关协议有开放式最短路径优先(OSPF,Open Shortest Path First)协议和寻路信息协议(RIP,Routing Information Protocol)。所谓自治系统,是指在同一实体(如学校、企业或 ISP)管理下的主机、路由器及其他网络设备的集合。

3.3.1　RIP 协议

RIP 是路由信息协议(Routing Information Protocol)的缩写，它采用距离向量算法，是当今应用最广泛的内部网关协议。在默认情况下，RIP 使用一种非常简单的度量制度：距离就是通往目的站点所需经过的链路数，取值为 1～15，数值 16 表示无穷大。RIP 进程使用 UDP 的 520 端口来发送和接收 RIP 分组。RIP 分组每隔 30s 以广播的形式发送一次，为了防止出现“广播风暴”，其后续的分组随机延时后发送。在 RIP 中，如果一条路由在 180s 内未被刷新，则相应的距离被设定成无穷大，并从路由表中删除该表项。RIP 分组分为两种：请求分组和响应分组。

RIP-1 提出较早，其中有许多缺陷。为了改善 RIP-1 的不足，在 RFC 1388 中提出了改进的 RIP-2，并在 RFC 1723 和 RFC 2453 中进行了修订。RIP-2 定义了一套有效的改进方案，支持子网路由选择、CIDR 和组播，并提供了验证机制。

RIP 协议简单、易于实施，可供大多数路由器免费使用。这些优点使 RIP 成为广受欢迎的路由协议。但 RIP 也有以下几个缺点：

① 支持的最大跳数为 15，因此应用 RIP 的网络不能串接 16 台以上的主机。

② 需定期发送路由表的完整副本到直接相连的邻居。在大型网络中，这可能导致每次更新时产生巨大的网络流量。

③ 大型网络发生改变时，网络收敛的速度很慢。

3.3.2　RIP 协议配置实例

为实现公司总部与分支机构的连接，通过广域网接口连接两个网络。为了简化操作，说明 RIP 的配置，将两个接口换为局域网口，分别为两台路由器的接口分配 IP 地址，并配置动态路由协议 RIP，这样，两个区域内的设备通过设置 IP 地址和网关就可以互相通信了。网络结构如图 3-5 所示。

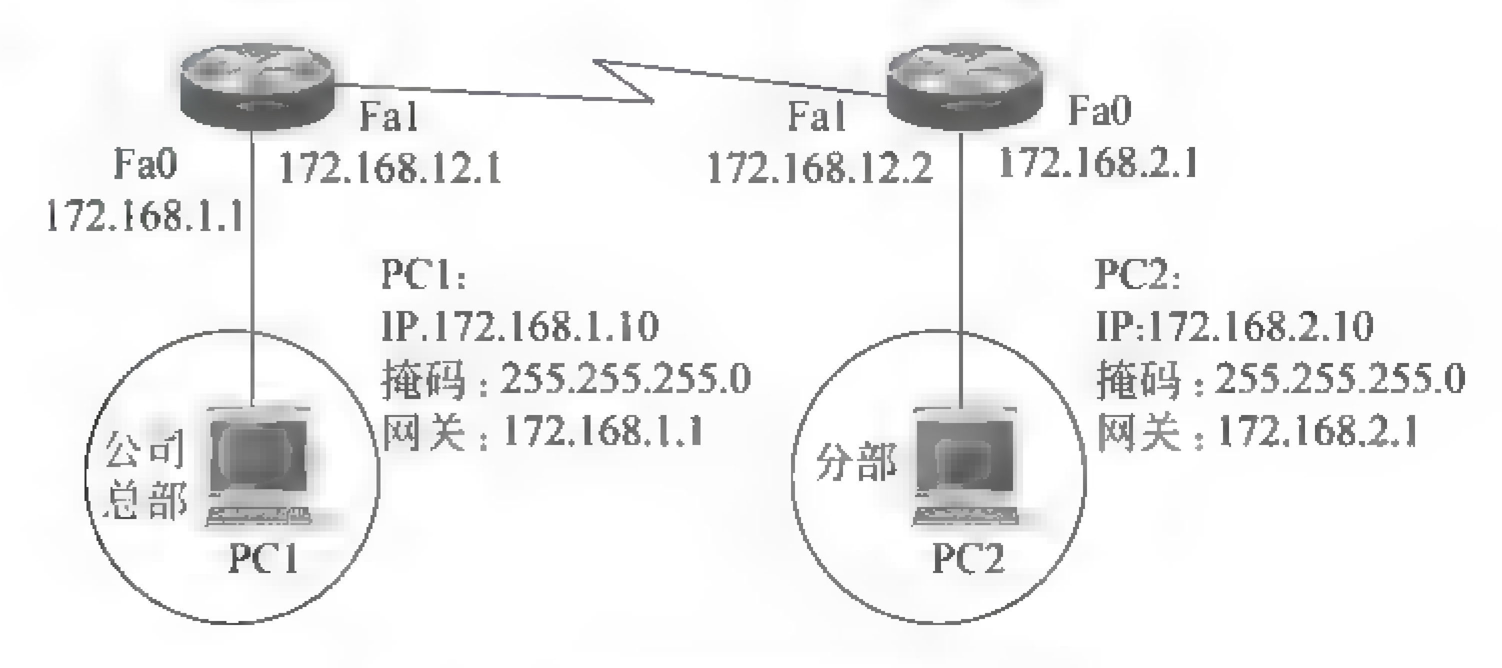


图 3-5　动态路由协议配置拓扑结构

(1) 左侧路由器配置

```
Hostname R1
```

```
Line vty 0 4
Login
Password 100
Exit
Enable password 100
Interface fastehternet 0
Ip address 172.16.1.1 255.255.255.0
No shutdown
Exit
Interface fastethernet 1
Ip address 172.16.12.1 255.255.255.0
Router rip
Network 172.16.1.0
Network 172.16.12.0
```

(2) 右侧路由器配置

```
Hostname R2
Line vty 0 4
Login
Password 100
Exit
Enable password 100
Interface fastehternet 0
Ip address 172.16.2.1 255.255.255.0
No shutdown
Exit
Interface fastethernet 1
Ip address 172.16.12.2 255.255.255.0
Router rip
Network 172.16.1.0
Network 172.16.12.0
```

配置完成后重启路由器，按图示将两台计算机的相关参数设置好。这两台机器之间如能互相 ping 通，说明 RIP 动态路由协议配置正确。

3.3.3 OSPF 协议

OSPF(Open Shortest Path First，开放式最短路径优先)是一个内部网关协议，用于在单一自治系统内决策路由。与 RIP 相对，OSPF 是链路状态路由协议，而 RIP 是距离向量路由协议。链路状态协议以其良好的分层设计和足以支持大型网络的可扩展性广泛应用于企业网络中并博得众多 ISP 的青睐。距离矢量协议通常不适合用在复杂的企业网络中。

1. OSPF 的起源

IETF 为了满足建造越来越大的基于 IP 网络的需要，形成了一个工作组，专门用于

开发开放式的链路状态路由协议，以便用在大型、异构的 IP 网络中。新的路由协议以已经取得成功的一系列私人的、和生产商相关的、最短路径优先(SPF)路由协议为基础。包括 OSPF 在内，所有的 SPF 路由协议基于一个数学算法——Dijkstra 算法。这个算法能使路由选择基于链路状态，而不是距离向量。OSPF 由 IETF 在 20 世纪 80 年代末期开发，是 SPF 类路由协议中的开放式版本。

链路是路由器接口的另一种说法，因此 OSPF 也称为接口状态路由协议。OSPF 通过路由器之间通告网络接口的状态来建立链路状态数据库，生成最短路径树，每个 OSPF 路由器使用这些最短路径构造路由表。

OSPF 路由协议一般用于同一个路由域内。在这里，路由域指一个自治系统(Autonomous System)，即 AS，是指一组通过统一路由政策或路由协议交换路由信息的网络。在这个 AS 中，所有的 OSPF 路由器都维护一个相同的描述该 AS 结构的数据库，该数据库中存放的是路由域中相应链路的状态信息。OSPF 路由器正是通过这个数据库计算出其 OSPF 路由表的。

作为一种链路状态的路由协议，OSPF 将链路状态广播数据包 LSA(Link State Advertisement)传送给在某一区域内的所有路由器，这一点与距离矢量路由协议不同。运行距离矢量路由协议的路由器是将部分或全部的路由表传递给与其相邻的路由器。

2. OSPF 的 Hello 协议

Hello 协议的作用如下：

① 用于发现邻居；

② 在成为邻居之前，必须对 Hello 包里的一些参数协商成功；

③ Hello 包在邻居之间扮演着 keepalive 的角色；

④ 允许邻居之间的双向通信；

⑤ 它在 NBMA(Nonbroadcast Multi-Access)网络上选举 DR 和 BDR。

3. OSPF 的网络类型

OSPF 定义的 5 种网络类型为：点到点网络、广播型网络、NBMA 网络、点到多点网络和虚链接(Virtual Link)。

① 点到点网络：如 T1 线路，是连接单独的一对路由器的网络。点到点网络上的有效邻居总是可以形成邻接关系。在这种网络上，OSPF 包的目标地址使用的是 224.0.0.5，这个组播地址称为 All SPF Routers。

② 广播型网络：如以太网、Token Ring 和 FDDI。这样的网络上会选举一个 DR 和 BDR，DR/BDR 发送的 OSPF 包的目标地址为 224.0.0.5，运载这些 OSPF 包的帧的目标 MAC 地址为 0100.5E00.0005。除了 DR/BDR 以外的 OSPF 包的目标地址为 224.0.0.6，这个地址叫做 All D Routers。

③ NBMA 网络：如 X.25、帧中继和 ATM，不具备广播的能力，因此邻居要人工指定。在这样的网络上要选举 DR 和 BDR，OSPF 包采用单播(unicast)的方式。

④ 点到多点网络：是 NBMA 网络的一个特殊配置，可以看成是点到点链路的集合。

在这样的网络上不选举 DR 和 BDR。

⑤ 虚链接：OSPF 包以单播(unicast)的方式发送。

所有网络可以归纳成两种网络类型，即传输网络（Transit Network）和末梢网络（Stub Network）。

4. OSPF 的 DR 和 BDR

在 DR 和 BDR 出现之前，每一台路由器和其邻居之间成为完全网状的 OSPF 邻接关系，这样，5 台路由器之间将形成 10 个邻接关系，同时产生 25 条 LSA。而且在多址网络中，还存在自己发出的 LSA 从邻居的邻居发回来，导致网络上产生很多 LSA 的复制的情况，所以产生了 DR 和 BDR。

DR 将完成如下工作：描述这个多址网络和该网络上的其他相关路由器；管理这个多址网络上的 Flooding(洪泛法)过程；为了冗余性，还会选取一个 BDR，作为双备份之用。

DR/BDR 选举是以接口状态机的方式触发的，其规则如下：

① 路由器的每个多路访问(multi-access)接口都有路由器优先级（Router Priority），这是个 8 位长的整数，范围是 0～255。Cisco 路由器默认的优先级是 1，优先级为 0 将不能选举为 DR/BDR。优先级可以通过命令“ip ospf priority”进行修改。

② Hello 包里包含了优先级的字段，还包括可能成为 DR/BDR 的相关接口的 IP 地址。

③ 当接口在多路访问网络上初次启动的时候，它把 DR/BDR 地址设置为 0.0.0.0，同时设置等待计时器(wait timer)的值等于路由器无效间隔(Router Dead Interval)。

DR/BDR 的选举过程如下所示：

① 在和邻居建立双向(2-Way)通信之后，检查邻居 Hello 包的优先级以及 DR 和 BDR 字段，列出所有可以参与 DR/BDR 选举的邻居。所有路由器声明它们自己就是 DR/BDR(Hello 包中 DR 字段的值就是它们自己的接口地址；BDR 字段的值就是它们自己的接口地址)。

② 从这个有参与选举 DR/BDR 权的列表中创建一组没有声明自己就是 DR 的路由器的子集(声明自己是 DR 的路由器将不会被选举为 BDR)。

③ 在这个子集里，不管有没有宣称自己就是 BDR，在 Hello 包中，BDR 字段就等于接口的地址，优先级最高的就被选举为 BDR；如果优先级都一样，RID 最高的被选举为 BDR。

④ 在 Hello 包中，DR 字段就等于接口的地址，优先级最高的就被选举为 DR；如果优先级都一样，RID 最高的选举为 DR；如果选出的 DR 不能工作，那么新选举的 BDR 成为 DR，再重新选举一个 BDR。

⑤ 注意，当网络中选举了 DR/BDR 后，又出现了 1 台新的优先级更高的路由器，DR/BDR 不会重新选举。

⑥ DR/BDR 选举完成后，所有路由器将组播 Hello 包到 All SPF Routers（地址 224.0.0.5)，以便它们能跟踪其他邻居的信息，即 DR 将洪泛 update packet(链路状态更

新包)到 224.0.0.5;DR other 只组播 update packet 到 All DRouter(地址 224.0.0.6),只有 DR/BDR 监听这个地址。

5. OSPF 区域

链路状态路由在设计时需要一个层次性的网络结构。OSPF 网络分为两个级别的层次,即骨干区域(backbone or area 0)和非骨干区域(nonbackbone areas)。

在一个 OSPF 区域中只能有一个骨干区域,可以有多个非骨干区域。骨干区域的区域号为 0。

各非骨干区域间是不可以交换信息的,它们只有与骨干区域相连,通过骨干区域交换信息。

非骨干区域和骨干区域之间相连的路由叫边界路由(ABR,Area Border Routers),只有 ABR 记载了各区域的所有路由表。各非骨干区域内的非 ABR 只记载本区域内的路由表,若要与外部区域中的路由相连,只能通过本区域的 ABR,由 ABR 连到骨干区域的 BR,再由骨干区域的 BR 连到要到达的区域。

骨干区域和非骨干区域的划分,大大减轻了区域内工作路由的负担。

6. OSPF 末梢区域

由于不是每台路由器都需要外部网络的信息,为了减少 LSA 泛洪量和路由表条目,创建了末梢区域,位于 Stub 边界的 ABR 将宣告一条默认路由到所有 Stub 区域的内部路由器。

7. OSPF 单域的基本配置命令

(1) 配置 LOOPBACK 接口地址

```
ROUTER(config)#interface loopbac k 0
ROUTER(config)#ip address IP 地址 掩码
```

(2) 启动 OSPF 路由进程

```
ROUTER(config)#router ospf 进程号
```

(3) 指定 OSPF 协议运行的接口和所在的区域

```
ROUTER(config)#network 网络号 反向掩码 AREA 区域号
```

(4) 修改接口的 COST 值

```
ROUTER(config)#ip ospf cost cost 值
```

(5) 查看邻居列表

```
ROUTER# show ip ospf neighbor
```

3.3.4 OSPF 协议配置实例

前面使用 RIP 动态路由协议进行了配置，在此仍以图 3 4 所示网络为例来配置 OSPF 动态路由协议。

(1) 左侧路由器配置

```
Hostname R1
Line vty 0 4
Login
Password 100
Exit
Enable password 100
Interface fastehternet 0
Ip address 172.16.1.1 255.255.255.0
No shutdown
Exit
Interface fastethernet 1
Ip address 172.16.12.1 255.255.255.0
Router ospf 1                                   !创建 OSPF 动态路由协议，并给予进程号"1"
Network 172.16.1.0 0.0.0.255 area 0             !宣布有哪些网络与该网络相连
Network 172.16.12.0 0.0.0.255 area 0
```

(2) 右侧路由器配置

```
Hostname R2
Line vty 0 4
Login
Password 100
Exit
Enable password 100
Interface fastehternet 0
Ip address 172.16.2.1 255.255.255.0
No shutdown
Exit
Interface fastethernet 1
Ip address 172.16.12.2 255.255.255.0
Router ospf 1
Network 172.16.1.0 0.0.0.255 area 0
Network 172.16.12.0 0.0.0.255 area 0
```

设置完成后重启路由器，可以按图示设置两台计算机的相关参数。两台机器之间如能互相 ping 通，说明 OSPF 动态路由协议配置正确。

任务3.4 PPP协议基本配置

3.4.1 PPP协议的工作原理

1. PPP协议的概念

点对点协议(PPP)为在点对点连接上传输多协议数据包提供了一个标准方法。PPP最初设计为两个对等节点之间的IP流量传输提供一种封装协议。在TCP/IP协议集中,它是一种用来同步调制连接的数据链路层(OSI参考模型中的第二层),替代了原来非标准的第二层协议,即SLIP。除了IP以外,PPP还可以携带其他协议,包括DECnet和Novell的Internet分组交换(IPX)。

2. PPP的工作原理

点对点协议(PPP)也是一种用于串行链路的数据链路层封装。它使用分层式体系结构来封装,并在一条点对点链路上承载多协议的数据报。由于PPP是基于标准的协议,它能够支持不同厂商设备之间的通信。

以下接口可支持PPP:异步串行接口、同步串行接口、高速串行接口(HSSI)和集成服务数字网络(ISDN)。

PPP有以下两个子协议:

① 链路控制协议:负责建立、维护和终止点对点链路。

② 网络控制协议:供不同的网络层协议进行交互。

PPP会话要经过三个阶段:链路建立、身份验证(可选)以及网络层协议。在PPP协议会话中可以选择是否对PPP链路执行身份验证。若配置了此功能,身份验证将发生在链路建立之后,网络层协议配置阶段开始之前。PPP链路上的身份验证分为两种类型,即口令验证协议(PAP)和挑战握手验证协议(CHAP)。

为了建立点对点链路通信,PPP链路的每一端必须首先发送LCP包,以便设定和测试数据链路。在链路建立,并且LCP所需的可选功能确定之后,PPP必须发送NCP包,以便选择和设定一个或更多个网络层协议。一旦每个被选择的网络层协议都被设定好,来自每个网络层协议的数据报就能在链路上发送了。

链路将保持通信设定不变,直到有LCP和NCP数据包关闭链路,或者是发生了外部事件(如休止状态的定时器期满,或者网络管理员干涉)。

3.4.2 PAP验证

1. PAP身份验证简介

PAP为远程设备提供了一种证实身份的简单方法。PAP使用双向握手来发送其用

户名和口令。被呼叫的设备将查找呼叫方设备的用户名，检查其发送的口令是否与数据库中存储的一致。如果两个口令匹配，则验证成功。

PAP以明文方式通过链路反复传送用户名/口令对，直到收到验证的确认信息或连接结束为止。此验证方法无法防止用户名和口令被数据包嗅探器(一种并联在网络中的监听网络数据包的设备，它可以是硬件也可以是软件)窃取。

此外，远程节点控制着登录尝试的频率和时间。一旦通过验证，远程设备上就不会再做任何查证。由于没有持续的验证机制，链路的已验证连接非常容易遭到劫持，黑客也可能通过重播攻击非法获得访问权。

2. PAP验证过程

PAP验证可以在一方进行，即由一方验证另一方身份；也可以进行双向身份验证，这时要求被验证的双方都要通过对方的验证程序，否则无法建立二者之间的链路。下面以单方认证为例，分析PAP配置过程及诊断方法，如图3-6所示。

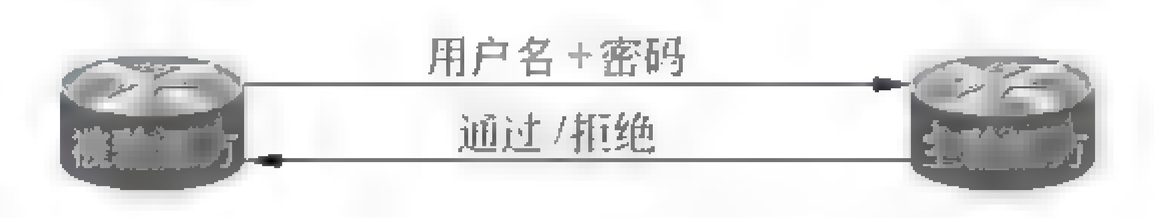


图3-6　PAP验证原理

3.4.3　PPP PAP验证过程配置实例

1. PPP PAP验证拓扑结构(如图3-7所示)

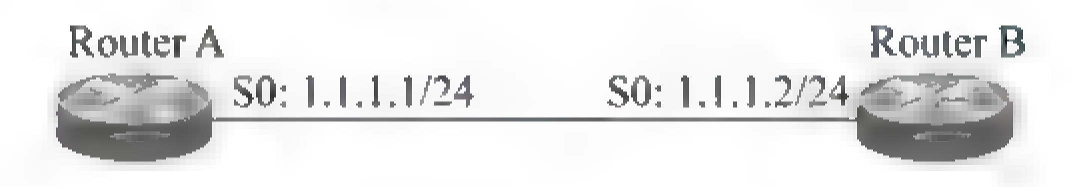


图3-7　PPP PAP验证拓扑结构

在PAP配置中，用户名为Red-Giant，设定密码Router，验证方的IP地址为1.1.1.1/24；被验证方的IP地址为1.1.1.2/24，要求设定的用户名和密码与验证方一样。Router A为被验证方，Router B为验证方。

2. 配置过程

① Router A配置

```
Red-Giant#config terminal
Red-Giant(config)#interface Serial0
!配置 IP 地址
Red-Giant(config-if)#ip address 1.1.1.2 255.255.255.0
!封装 PPP 协议
Red-Giant(config-if)#encapsulation ppp
```

```
Red-Giant(config-if)#bandwidth 2000000
Red-Giant(config-if)#clock rate 64000
!设置 PAP 验证的用户名和密码
Red-Giant(config-if)#ppp pap sent-username Red-Giant password 0 Router
```

② Router B 配置

```
Red-Giant#config terminal
Red-Giant(config)#username Red-Giant password 0 Router
Red-Giant(config)#interface Serial0
!配置 IP 地址
Red-Giant(config-if)#ip address 1.1.1.1 255.255.255.0
!封装 PPP 协议
Red-Giant(config-if)#encapsulation ppp
!设定 PPP 的验证方式
Red-Giant(config-if)#ppp authentication pap
```

3. 验证命令

```
Show interface Serial0
Debug ppp authentication
```

3.4.4　CHAP 验证

1. CHAP 验证简介

CHAP 验证是一种比 PAP 验证更安全的身份验证过程。CHAP 不会在链路上发送明文口令，不仅初次建立连接时会进行身份验证，在链路活动期间还将反复进行身份验证。身份验证的频率和时机由被叫设备控制，因此劫持攻击几乎不可能实现。

CHAP 使用三次握手验证（如图 3-8 所示），其验证过程如下：



图 3-8　CHAP 三次握手验证

① 主验证方向被验证方发送一些随机产生的数据包，同时附带本方主机名一起发送给被验证方。

② 被验证方接收到对方发送的验证请求（Challenge）时，根据此数据包中的主验证方的主机名和本方的用户数据库查找用户口令。如果找到用户数据库中与主验证方主机名相同的用户，便利用接收到的随机数据包和主验证方的密钥，采用 MD5 算法生成应答，将应答和自己的主机名送回。

③ 主验证方接收到应答后，利用对方的用户名在自己的用户数据库中查找本方保留的口令，根据本方保留的密钥和随机报文，采用 MD5 算法得出结果，与被验证方应答比较，返回相应的结果。

CHAP 对端系统要求很高，因为需要进行多次身份质询、响应，这将耗费较多的 CPU 资源，因此只用在对安全要求很高的场合。

2. CHAP 验证服务器的配置

CHAP 验证服务器的配置分为两个步骤：建立本地口令数据库和要求进行 CHAP 验证。

(1) 建立本地口令数据库

通过全局模式下的命令"username username password password"来为本地口令数据库添加记录。请注意，此处的 username 应该是对端路由器的名称，即 routerb，如下所示：

```
RouterA(config)#username routerb password samepass
```

(2) 要求进行 CHAP 验证

这需要在相应接口配置模式下使用命令"ppp authentication chap"来完成，如下所示：

```
RouterA(config)#interface serial 0/0
RouterA(config-if)#ppp authentication chap
```

3. CHAP 验证客户端的配置

CHAP 验证客户端的配置只需要一个步骤(命令)，即建立本地口令数据库。请注意，此处的 username 应该是对端路由器的名称，即 routera，口令应该和 CHAP 验证服务器口令数据库中的口令相同，如下所示：

```
RouterB(config-if)#username routera password samepass
```

3.4.5 PPP CHAP 验证过程配置实例

1. PPP CHAP 验证拓扑结构(如图 3-9 所示)



图 3-9 PPP CHAP 验证拓扑结构

对于 PPP CHAP 验证的配置，Router A 为验证方，IP 地址为 1.1.1.1/24，主机名为 Router A，要求口令为 Router，建立的用户列表中包括 Router B 的主机名；Router B 为验证方，IP 地址为 1.1.1.2/24，主机名为 Router B，口令发送为 Router。

2. 配置过程

① Router A 配置

```
Red-Giant#config terminal
!设置主机名
Red-Giant(config)#hostname RouterA
```

```
!设置用户名和密码的列表
RouterA(config)#username RouterB password 0 Router
RouterA(config)#username RouterC password 0 Router
RouterA(config)#interface serial0
!封装协议
RouterA(config-if)#encap ppp
RouterA(config-if)#bandwidth 2000000
RouterA(config-if)#clock rate 64000
!设置 IP 地址
RouterA(config-if)#ip address 1.1.1.1 255.255.255.
RouterA(config-if)#ppp chap hostname RouterA
RouterA(config-if)#ppp chap password 0 Router
```

② Router B 配置

```
Red-Giant(config)#hostname RouterB
!以对方的主机名作为用户名,密码和对方路由器的密码设定一致
RouterB(config)#username RouterA password 0 Router
RouterB(config)#interface serial0
!封装协议
RouterB(config-if)#encap ppp
RouterB(config-if)#ppp auth chap!设置 IP 地址
RouterB(config-if)#ip address 1.1.1.2 255.255.255.0
```

3. 验证命令

```
Show interface Serial0
Debug ppp authentication
```

任务 3.5　NAT 地址转换基本配置

计算机接入互联网时,必须具有唯一的 IP 地址。然而随着网络的普及,可用的 IPv4 地址已经远远不能满足需求。尽管 IPv6 可以解决这个问题,但在将 IPv6 全部实施到 Internet 上还需要一些时间。目前,网络地址转换(NAT,Network Address Translation)是用来解决 IP 地址不足的重要手段。

3.5.1　NAT 实现方式

NAT 的实现方式有三种,即静态 NAT、动态 NAT 和端口多路复用。

静态转换是指将内部网络的私有 IP 地址转换为公有 IP 地址。将一个内部本地地址映射为一个全局或公有地址。这样的映射可确保特定的内部本地地址始终与同一个公有地址相关联。静态 NAT 可确保外部设备始终能到达内部设备。例如,向外界开放的 Web 服务器和 FTP 服务器。

动态转换是指将内部网络的私有 IP 地址转换为公用 IP 地址时，IP 地址对是不确定的，是随机的，所有被授权访问 Internet 的私有 IP 地址可随机转换为任何指定的合法 IP 地址。也就是说，只要指定哪些内部地址可以转换，以及用哪些合法地址作为外部地址，就可以进行动态转换。动态转换可以使用多个合法外部地址集。当 ISP 提供的合法 IP 地址略少于网络内部的计算机数量时，可以采用动态转换方式。

端口多路复用(PDM，Port Division Multiplexing)是指改变外出数据包的源端口并进行端口转换，即端口地址转换(PAT，Port Address Translation)。采用端口多路复用方式，内部网络的所有主机均可共享一个合法外部 IP 地址实现对 Internet 的访问，从而最大限度地节约 IP 地址资源。同时，可隐藏网络内部的所有主机，有效避免来自 Internet 的攻击。因此，目前网络中应用最多的就是端口多路复用方式。

3.5.2　网络地址转换(NAT)的实现

在网络地址转换之前，首先必须搞清楚内部接口和外部接口，以及在哪个外部接口上启用 NAT。通常情况下，连接到用户内部网络的接口是 NAT 内部接口，连接到外部网络(如 Internet)的接口是 NAT 外部接口。

1. 静态地址转换的实现

假设内部局域网使用的 IP 地址段为 172.16.0.1～172.168.0.254，路由器局域网端口(即默认网关)的 IP 地址为 172.168.0.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 61.159.62.128～61.159.62.135，路由器在广域网中的 IP 地址为 61.159.62.129，子网掩码为 255.255.255.248，可用于转换的 IP 地址范围为 61.159.62.130～61.159.62.134。要求将内部网址 172.16.0.2～172.168.0.6 分别转换为合法 IP 地址 61.159.62.130～61.159.62.134。

第一步，设置外部端口。

```
interface serial 0
ip address 61.159.62.129 255.255.255.248
ip nat outside
```

第二步，设置内部端口。

```
interface ethernet 0
ip address 192.168.0.1 255.255.255.0
ip nat inside
```

第三步，在内部本地地址与内部合法地址之间建立静态地址转换。

```
ip nat inside source static 内部本地地址 内部合法地址
```

示例：

```
ip nat inside source static 192.168.0.2 61.159.62.130
                     !将内部网络地址 192.168.0.2 转换为合法 IP 地址 61.159.62.130
```

```
ip nat inside source static 192.168.0.3 61.159.62.131
                                   !将内部网络地址 192.168.0.3转换为合法 IP地址 61.159.62.131
ip nat inside source static 192.168.0.4 61.159.62.132
                                   !将内部网络地址 192.168.0.4转换为合法 IP地址 61.159.62.132
ip nat inside source static 192.168.0.5 61.159.62.133
                                   !将内部网络地址 192.168.0.5转换为合法 IP地址 61.159.62.133
ip nat inside source static 192.168.0.6 61.159.62.134
                                   !将内部网络地址 192.168.0.6转换为合法 IP地址 61.159.62.134
```

2. 动态地址转换的实现

假设内部网络使用的 IP 地址段为 172.16.100.1～172.16.100.254，路由器局域网端口(即默认网关)的 IP 地址为 172.16.100.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 61.159.62.128～61.159.62.191，路由器在广域网中的 IP 地址为 61.159.62.129，子网掩码为 255.255.255.192，可用于转换的 IP 地址范围为 61.159.62.130～61.159.62.190。要求将内部网址 172.16.100.1～172.16.100.254 动态转换为合法 IP 地址 61.159.62.130～61.159.62.190。

第一步，设置外部端口。

设置外部端口命令的语法如下：

```
ip nat outside
```

示例：

```
interface serial 0              !进入串行端口 serial 0
ip address 61.159.62.129 255.255.255.248
                                   !将其 IP 地址指定为 61.159.62.129,子网掩码为 255.255.255.248
ip nat outside                  !将串行口 serial 0设置为外网端口.可以定义多个外部端口
```

第二步，设置内部端口。

设置内部接口命令的语法如下：

```
ip nat inside
```

示例：

```
interface ethernet 0            !进入以太网端口 Ethernet 0
ip address 172.16.100.1 255.255.255.0
                                   !将其 IP 地址指定为 172.16.100.1,子网掩码为 255.255.255.0
ip nat inside                   !将 Ethernet 0设置为内网端口.可以定义多个内部端口
```

第三步，定义合法 IP 地址池。

定义合法 IP 地址池命令的语法如下：

```
ip nat pool 地址池名称 起始 IP地址 终止 IP地址 子网掩码
```

其中，地址池名字可以任意设定。

示例：

```
ip nat pool net 61.159.62.130 61.159.62.190 netmask 255.255.255.192
```

指明地址缓冲池的名称为 net，IP 地址范围为 61.159.62.130～61.159.62.190，子网掩码为 255.255.255.192。需要注意的是，即使掩码为 255.255.255.0，也会由起始 IP 地址和终止 IP 地址对 IP 地址池进行限制。

```
ip nat pool test 61.159.62.130 61.159.62.190 prefix-length 26
```

如果有多个合法 IP 地址范围，可以分别添加。例如，如果还有一段合法 IP 地址范围为 211.82.216.1～211.82.216.254，那么，可以再通过下述命令将其添加至缓冲池：

```
ip nat pool cernet 211.82.216.1 211.82.216.254 netmask 255.255.255.0
```

或

```
ip nat pool test 211.82.216.1 211.82.216.254 prefix- length 24
```

第四步，定义内部网络中允许访问 Internet 的访问列表。

定义内部访问列表命令的语法如下：

```
access-list1 标号 permit 源地址 通配符
```

其中，“标号”为 1～99 之间的整数。

```
access-list1 permit 172.16.100.0 0.0.0.255
```

允许访问 Internet 的网段为 172.16.100.0～172.16.100.255，主机掩码为 0.0.0.255。需要注意的是，这里采用的是主机掩码，而非子网掩码。子网掩码与主机掩码的关系为：主机掩码+子网掩码=255.255.255.255。例如，子网掩码为 255.255.0.0，则主机掩码为 0.0.255.255；子网掩码为 255.0.0.0，则主机掩码为 0.255.255.255；子网掩码为 255.252.0.0，则主机掩码为 0.3.255.255；子网掩码为 255.255.255.192，则主机掩码为 0.0.0.63。

另外，如果想将多个 IP 地址段转换为合法 IP 地址，可以添加多个访问列表。例如，当欲将 172.16.98.0～172.16.98.255 和 172.16.99.0～172.16.99.255 转换为合法 IP 地址时，应当添加下述命令：

```
access-list2 permit 172.16.98.0~0.0.0.255
access-list2 permit 172.16.99.0~0.0.0.255
```

第五步，实现网络地址转换。

在全局设置模式下，将由 access list 指定的内部本地地址与指定的内部合法地址池进行地址转换。命令语法如下：

```
ip nat inside source list 访问列表标号 pool 内部合法地址池名字
```

示例：

```
ip nat inside source list 1 pool chinanet
```

如果有多个内部访问列表，可以一一添加，以实现网络地址转换，例如：

```
ip nat insde source list 2 pool chinanet
ip nat insde source list 2 pool chinanet
```

如果有多个地址池，也可以一一添加，以增加合法地址池范围，例如：

```
ip nat insde source list 2 pool cernet
ip nat insde source list 2 pool cernet
ip nat insde source list 2 pool cernet
```

3. 端口复用动态地址转换(PAT)

内部网络使用的 IP 地址段为 10.100.100.1～10.100.100.254，路由器局域网端口(即默认网关)的 IP 地址为 10.100.100.1，子网掩码为 255.255.255.0。网络分配的合法 IP 地址范围为 202.130.100.0～202.130.100.3，路由器广域网中的 IP 地址为 202.130.100.1，子网掩码为 255.255.255.252，可用于转换的 IP 地址为 202.130.100.2。要求将内部网址 10.100.100.1～10.100.100.254 转换为合法 IP 地址 202.130.100.2。

第一步，设置外部端口。

```
interface serial 0
ip address 202.130.100.1 255.255.255.252
in nat outside
```

第二步，设置内部端口。

```
interface ethernet 0
ip address 10.100.100.1 255.255.255.0
ip nat inside
```

第三步，定义合法 IP 地址池。

```
in nat pool onlyone 202.130.100.2 202.130.100.2 netmask 255.255.255.252
```

指明地址缓冲池的名称为 onlyone，IP 地址范围为 202.130.100.2，子网掩码为 255.255.255.252。由于本例只有一个 IP 地址可用，所以起始 IP 地址与终止 IP 地址均为 202.130.100.2。如果有多个 IP 地址，则应当分别输入起止的 IP 地址。

第四步，定义内部访问列。

```
access-list 1 permit 10.100.100.0 0.0.0.255
```

允许访问 Internet 的网段为 10.100.100.0～10.100.100.255，子网掩码为 255.255.255.0。需要注意的是，在这里，子网掩码的顺序跟平常所写的顺序相反，即 0.255.255.255。

第五步，设置复用动态地址转换。

在全局设置模式下，在内部本地地址与内部合法 IP 地址间建立复用动态地址转换。命令语法如下：

```
ip nat inside source list 访问列表号 pool 内部合法地址池名字 overload
```

示例：

```
ip nat inside source list1 pool onlyone overload
```

以端口复用方式，将访问列表1中的私有IP地址转换为onlyone IP地址池中定义的合法IP地址。

3.5.3 网络地址转换(NAT)的配置实例

1. 全部采用端口复用地址转换

当ISP分配的IP地址数量很少，网络又没有其他特殊需求，即无须为Internet提供网络服务时，可采用端口复用地址转换方式，使网络内的计算机采用同一个IP地址访问Internet，在节约IP地址资源的同时，又可有效保护网络内部的计算机。

(1) 网络拓扑环境(如图3-10所示)

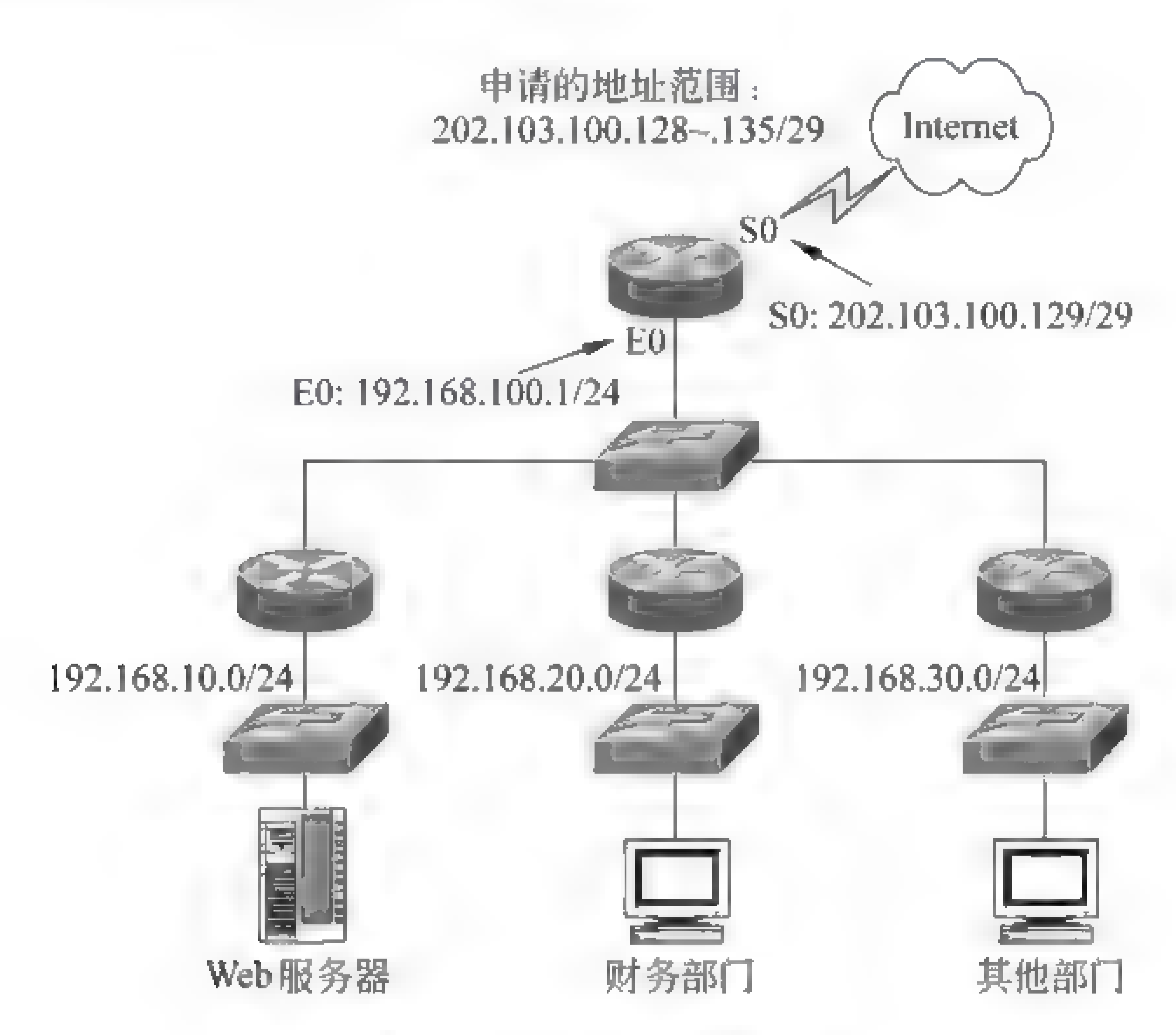


图3-10 NAT地址转换

局域网采用100Mbps光纤，以城域网方式接入Internet。路由器选用拥有2个10/100Mbps自适应端口的Cisco 2611。内部网络使用的IP地址段为192.168.100.1~192.168.101.254，局域网端口Ethernet 0的IP地址为192.168.100.1，子网掩码为255.255.0.0。网络分配的合法IP地址范围为202.130.100.128~202.130.100.131，连接ISP的端口Ethernet 1的IP地址为202.130.100.129，子网掩码为255.255.255.252。可用于转换的IP地址为202.130.100.130。要求网络内部的所有计算机均可访问Internet。

(2) 任务分析

既然只有一个可用的合法IP地址，处于局域网的服务器又只为局域网提供服务，而不允许Internet中的主机对其访问，因此完全可以采用端口复用地址转换方式实现NAT，使得网络内的所有计算机均可独立访问Internet。

(3) 命令配置

```
interface fastethernet0/0
ip address 192.168.100.1 255.255.0.0                    !定义本地端口 IP 地址
duplex auto
speed auto
ip nat inside                                            !定义为本地端口
interface fastethernet0/1
ip address 202.130.100.129 255.255.255.252
duplex auto
speed auto
ip nat outside
ip nat pool onlyone 202.130.100.130 202.130.100.130 netmadk 255.255.255.252
                                                          !定义合法 IP 地址池,名称为 onlyone
access-list 1 permit 192.168.100.0 0.0.0.255              !定义本地访问列表
access-list 1 permit 192.168.100.0 0.0.0.255
ip nat inside source list1 pool onlyone overload          !采用端口复用动态地址转换
```

2. 动态地址十端口复用地址转换

许多 FTP 网站考虑到服务器性能和 Internet 连接带宽的占用问题,都限制同一个 IP 地址的多个进程访问。如果采用端口复地址转换方式,则网络内的所有计算机都采用同一个 IP 地址访问 Internet,将因此被禁止对该网站的访问。所以,当提供的合法 IP 地址数量稍多时,可同时采用端口复用和动态地址转换方式,既可保证所有用户都能够获得访问 Internet 的权利,又不致某些计算机因使用同一个 IP 地址而被限制权限。需要注意的是,由于所有计算机都采用动态地址转换方式,因此 Internet 中的所有计算机将无法实现对网络内部服务器的访问。

(1) 网络拓扑环境

局域网以 2Mbps DNA 专线接入 Internet,路由器选用安装了广域网模块的 Cisco 2611,如图 3-10 所示(IP 地址有相应的变化)。内部网络使用的 IP 地址段为 172.16.100.1~172.16.102.254,局域网端口 Ethernet 0 的 IP 地址为 172.16.100.1,子网掩码为 255.255.0.0。网络分配的合法 IP 地址范围为 202.130.100.128~202.130.100.129,子网掩码为 255.255.255.192,可用于转换的 IP 地址范围为 202.130.100.130~202.130.100.190。要求网络部分的部分计算机可以不受任何限制地访问 Internet,服务器无须提供 Internet 访问服务。

(2) 任务分析

既然要求网络中的部分计算机可以不受任何限制地访问 Internet,同时,服务器无须提供 Internet 访问服务,那么,只需采用动态地址转换+端口复用地址转换方式即可实现。部分有特殊需求的计算机采用动态地址转换的 NAT 方式,其他计算机则采用端口复用地址转换的 NAT 方式。因此,部分有特殊需求的计算机可采用内部网址 172.16.100.1~172.16.100.254,并动态转换为合法地址 202.130.100.130~202.130.100.189,其他计算机采用内部网址 172.16.101.1~172.16.102.254,全部转换为 202.

130.100.190。

(3) 命令配置

```
interface fastethernet0/1
ip address 10.100.100.1 255.255.255.0              !定义局域网端口 IP 地址
duplex auto
speed auto
ip nat inside                                      !定义为局域端口
!
interface serial 0/0
ip address 202.130.100.129 255.255.255.192         !定义广域网端口 IP 地址
!
duplex auto
speed auto
ip nat outside                                     !定义为广域端口
!
ip nat pool public 202.130.100.130 202.130.160.190 netmask 255.255.255.192
                                                   !定义合法 IP 地址池,名称为 public
ip nat pool super 202.130.100.130 202.130.160.189 netmask 255.255.255.192
                                                   !定义合法 IP 地址池,名称为 super
ip nat inside source list1 pool super              !定义列表 1 采用动态地址转换
ip nat inside source list2 pool public overload?   !定义列表 2 采用端口复用地址转换
access-list1 permit 172.16.100.0 0.0.0.255         !定义本地访问列表 1
access-list2 permit 172.16.102.0 0.0.0.255         !定义本地访问列表 2
access-list2 permit 172.16.102.0 0.0.0.255
```

3. 静态地址转换+端口复用地址转换

其实在很多时候，网络中的服务器既为网络内部的客户提供网络服务，又同时为Internet中的用户提供访问服务。因此，如果采用端口复用地址转换或动态地址转换，将由于无法确定服务器的IP地址，而导致Internet用户无法实现对网络内部服务器的访问。此时，应当采用静态地址转换+端口复用地址转换的NAT方式。也就是说，对服务器采用静态地址转换，以确保服务器拥有固定的合法IP地址；对普通的客户计算机采用端口复用地址转换，使所有用户都享有访问Internet的权利。

(1) 网络拓扑环境

局域网采用10Mbps光纤，以城域网方式接入Internet，如图3-9所示(IP地址有相应的变化)。路由器选用拥有2个10/100Mbps自适应端口的Cisco 2611。内部网络使用的IP地址段为10.18.100.1～10.18.104.254，局域网端口Ethernet 0的IP地址为10.18.100.1，子网掩码为255.255.0.0。网络分配的合法IP地址范围为211.82.220.80～211.82.220.87，连接ISP的端口Ethernet 1的IP地址为211.82.220.81，子网掩码为255.255.255.248。要求网络内部的所有计算机均可访问Internet，并且在Internet中提供Web，E-mail，FTP和Media 4种服务。

(2) 任务分析

既然网络内的服务器要求能够被Internet访问到，那么，这部分主机必须拥有合法的

IP 地址，也就是说，服务器必须采用静态地址转换。其他计算机由于没有任何限制，所以可采用端口复用地址转换的 NAT 方式。因此，服务器可采用内部网址 10.18.100.1～10.18.100.254，并分别映射为一个合法的 IP 地址。其他计算机则采用内部网址 10.18.101.1～172.16.104.254，并全部转换为一个合法的 IP 地址。

(3) 命令配置

```
interface fastethernet0/0
ip address 10.18.100.1 255.255.0.0              !定义局域网口 IP 地址
duplex auto
speed auto
ip nat inside                                   !定义局域网口
interface fastethernet0/1
ip address 211.82.220.81 255.255.255.248        !定义广域网口 IP 地址
duplex auto
speed auto
ip nat outside                                  !定义广域网口
ip nat pool every 211.82.220.86 211.82.220.86 netmask 255.255.255.248
access-list 1 permit 10.18.101.0 0.0.0.255      !定义本地访问列表 1
access-list 1 premit 10.18.102.0 0.0.0.255
access-list 1 premit 10.18.103.0 0.0.0.255
access-list 1 premit 10.18.104.0 0.0.0.255
ip nat inside source list1 pool every overload  !定义列表 1 采用端口复用地址转换
ip nat inside source static 10.18.100.10 211.82.220.82        !定义静态地址转换
ip nat inside source static 10.18.100.11 211.82.220.83
ip nat inside source static 10.18.100.12 211.82.220.84
ip nat inside source static 10.18.100.13 211.82.220.85
```

规律总结(检查)

路由是把信息从源通过网络传递到目的地的行为，在路上，至少遇到一个中间节点。路由通常与桥接来对比，在粗心的人看来，它们完成的是同样的事。其主要区别在于桥接发生在 OSI 参考模型的第二层(数据链路层)，路由发生在第三层(网络层)。这一区别使二者在传递信息的过程中使用不同的信息，以不同的方式完成任务。

1. 路由器工作任务描述

路由器最根本的任务就是数据转发。换言之，路由器所做的工作就是两大项：转发什么和怎样转发的问题。

路由器转发的对象是那些按照某种“被路由协议”组织的、可寻址的数据包。

路由器转发的依据是“路由表”，从路由表中查找数据包的转发路径。路由表是按照“路由选择协议”建立和维护的。

2. 路由器主要协议配置常用命令

路由器主要协议配置常用命令及功能如表 3-1 所示。

表 3-1 路由器主要协议配置常用命令及功能

项 目	命 令	功 能
静态路由配置	ip route network mask{ip-address | interface-type interface-number}[distace][permanent]	配置静态路由
	no ip route network mask	删除静态路由
动态路由配置—RIP	Router rip	创建 RIP 路由进程
	Network network-number	定义关联网络
动态路由配置—OSPF	Router ospf process-id	创建 OSPF 路由进程
	Network network wildcard area area-id	定义接口所属区域
PAP 被验证方	Ppp pap sent-username username password password	指定 PPP PAP 验证的用户名和密码
	no ppp pap sent-username	取消 PPP PAP 验证的设定
PAP 验证方	ppp authentication pap	设定 PPP PAP 验证方
	username username password password	创建用户数据库记录
CHAP 被验证方	ppp chap hostname hostname	指定 PPP CHAP 验证主机名
	ppp chap password password	指定 PPP CHAP 验证的密码
CHAP 验证方	ppp authentication chap	启动 PPP CHAP 验证方式
	username username password password	创建用户数据库记录
	no ppp authentication chap	取消 CHAP 验证方式

3. 网络地址转换

路由器的网络地址转换功能很好地为当前私有网络解决了地址不足的问题，成为当前私有网络接入 Internet 的主要手段，其转换功能主要体现在以下三个方面：

① 静态网络地址转换将单个内部私有地址映射为单个公有地址；

② 动态网络地址转换使用可用的公有地址池，并将它们分配给内部私有地址；

③ 端口多路复用将多个内部私有地址转换为单个公有地址。

拓展提高(拓展)

1. 有类寻址与无类寻址

1981 年以前，IP 地址仅使用前 8 位来指定地址中的网络部分，因而 Internet(那时称为 ARPANET)的范围仅限于 256 个网络。很快，地址空间便不能满足人们的需求。

到 1981 年，RFC791 修改了 IPv4 的 32 位地址，将网络分为三种不同的类别：A 类、B 类和 C 类，每种类别的规模各不相同。A 类地址的网络部分使用 8 位，B 类地址的网络部分使用 16 位，C 类地址的网络部分使用 24 位。此格式就是人们所熟知的有类 IP 寻址。

最初发展形成的有类寻址方式在一段时间内解决了 256 个网络的限制问题。而十

年之后，IP 地址空间再度面临快速耗尽的危险，而且形势越来越严峻。为此，IETF（Internet 工程工作小组）引入了 CIDR（无类域间路由）技术，使用 VLSM（可变长子网掩码）来节省地址空间。

通过使用 CIDR 和 VLSM，ISP 可以将一个有类网络划分为不同的部分，从而分配给不同的客户使用。随着 ISP 开始采用不连续编址方式，无类路由协议随之产生。比较而言，有类路由协议总是在有类网络边界处总结，且其路由更新中不包含子网掩码信息。无类路由协议则在路由更新中包含子网掩码信息，并且不需要执行子网总结。

有类路由协议包括 RIPv1；无类路由协议包括 RIPv2，EIGRP 和 OSPF。

2. Cisco 路由器的接口类型

Cisco 路由器就像计算机一样，有自己的 CPU 和 RAM；还有的路由器是“模块化的”，就像计算机上的插槽一样，想实现什么功能，将相应的模块插到插槽即可。现在有两种接口的路由器：固定模块的路由器和模块化的路由器。

① 固定模块的路由器：这种路由器没有扩展插槽。买来的设备带什么接口，就是什么接口，不能添加新的模块。Cisco 2500 系列以下（包括 2500 系列）的路由器，例如 1600/1700 系列、700/800 系列，都是固定模块的路由器。

② 模块化的路由器：这种路由器配有可扩展插槽，想要实现什么功能，将相应的模块插入插槽即可。Cisco 2600 系列以上（包括 2600 系列）的路由器，例如 2600 系列、3600 系列，都是模块化的路由器。另外，对于模块化的路由器来讲，有些模块可能比路由器本身还要贵。

3. Cisco 路由器接口的表示法

对于模块化和非模块化的路由器，其接口表示方法是不同的。

(1) 固定模块的接口

固定模块的接口可以“接口名称+接口编号”的模式来表示，比如对于某台路由器的一个串口，可以用 Serial 1 来表示。注意，第一个接口的起始编号是从 0 开始的，也就是说，对于路由器的第一个串口，用 Serial 0 表示，第二个用 Serial 1 表示，……，以此类推；而对于这个路由器的第一个以太口，用 Ethernet 0 表示，第二个用 Ethernet 2 表示，……，以此类推。以下是常用接口的名称：

- 串口：Serial
- 以太口：Ethernet
- ISDN BRI 接口：BRI
- 管理控制台接口：Console

(2) 模块化的接口

模块化接口的表示法是“接口名称+接口所在的扩展槽号码/接口号码”。比如，对于某台路由器的一个扩展槽的第一个串口，用 Serial 0/0 表示。注意，扩展槽编号也是从 0 开始的。同理，对于路由器第二个扩展槽的第二个以太口，可以表示成 Ethernet 1/1。

另外，接口的名称可以简写，串口可以简写为 S，以太口可以简写为 E，但有些是不能简写的。

4. 路由器与三层网络设备

路由器的主要用途是连接多个网络，并将数据包转发到自身的网络或其他网络。由于路由器的主要转发决定是根据第三层 IP 数据包(即根据目的 IP 地址)做出的，因此路由器被视为第三层设备。作出决定的过程称为路由。

每个路由器在收到数据包后，都会搜索自身的路由表，寻找数据包目的 IP 地址与路由表中网络地址的最佳匹配。如果找到匹配项，就将数据包封装到对应外发接口的第二层数据链路帧中。数据链路封装的类型取决于接口的类型，如以太网接口或 HDLC 接口。最后，数据包到达与目的 IP 地址相匹配的网络中的路由器。

路由器在第三层做出主要转发决定，但正如我们前面所分析的，它也参与第一层和第二层的过程。路由器检查完数据包的 IP 地址，并通过查询路由表做出转发决定后，将该数据包从相应接口朝着目的地转发出去。路由器会将第三层 IP 数据包封装到对应送出接口的第二层数据链路帧的数据部分。帧的类型可以是以太网、HDLC 或其他第二层封装，即对应特定接口上所使用的封装类型。第二层帧会编码成第一层物理信号，这些信号用于表示物理链路上传输的位。路由器转发数据包流程如图 3-11 所示。

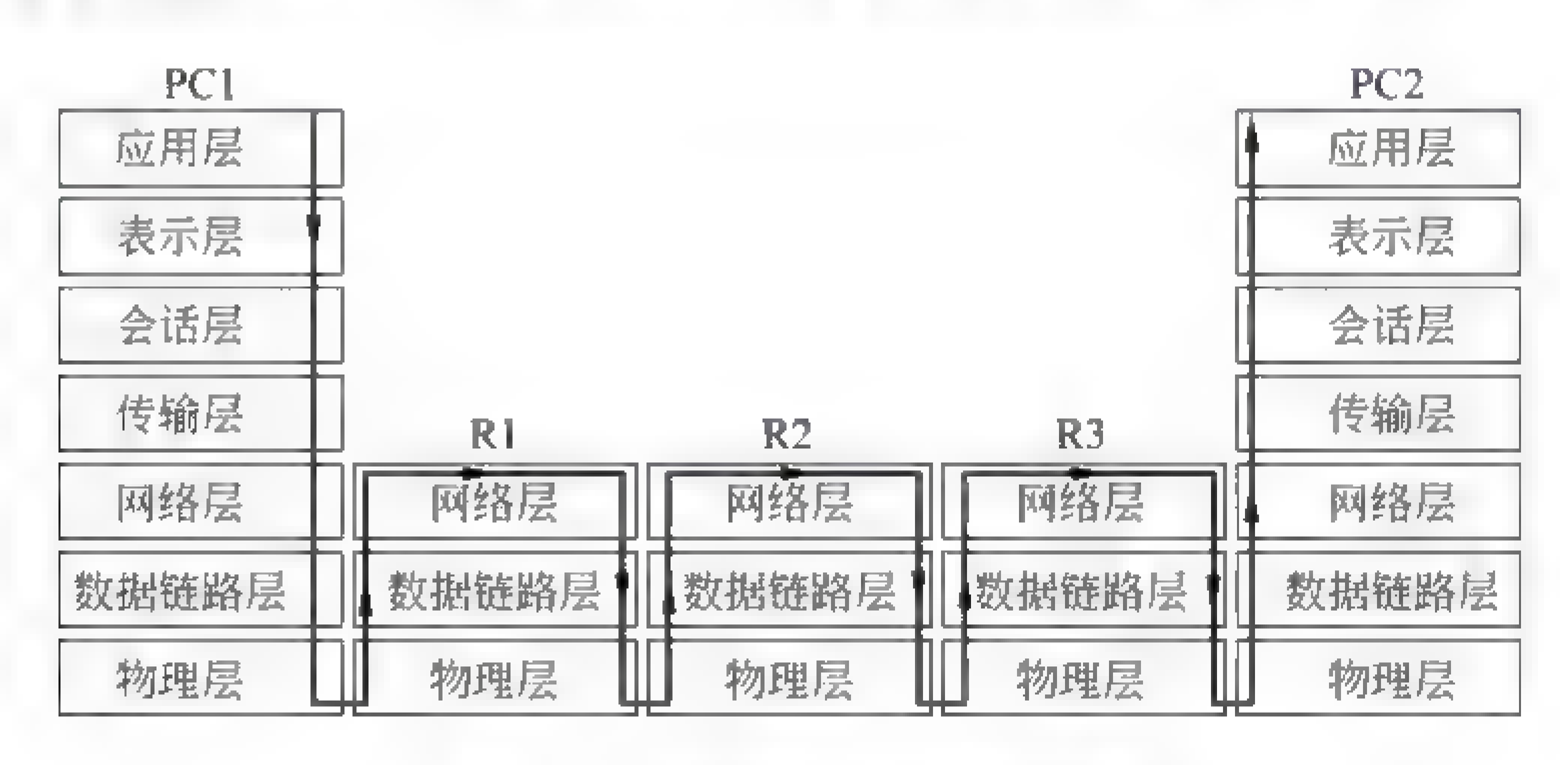


图 3-11 路由器转发数据包流程

(1) 路由与桥接

路由相对于二层的桥接/交换是高层的概念，不涉及网络的物理细节。在可路由的网络中，每台主机都有同样的网络层地址格式(如 IP 地址)，而无论它是运行在以太网、令牌环网、FDDI 网还是广域网。网络层地址通常由两部分构成：网络地址和主机地址。

网桥只能连接数据链路层相同(或类似)的网络，路由器则不同，它可以连接任意两种网络，只要主机使用的是相同的网络层协议。

(2) 连接网络层与数据链路层

网络层下面是数据链路层，为了它们可以互通，需要“黏合”协议。ARP(地址解析协议)用于把网络层(三层)地址映射到数据链路层(二层)地址，RARP(反向地址解析协议)则反之。

虽然 ARP 的定义与网络层协议无关，但它通常用于解析 IP 地址。最常见的是在数据链路层相同或类似的网络中应用，例如以太网，因此下面有关 ARP 和 RARP 的例子是基于 IP 和以太网提出的，这些概念对其他协议也是一样的。

路由是路由器最基本的功能。在 HOS 软件系统中，我们采用控制与转发分离的技术。路由协议作为控制信令的协议，负责计算路由，转发引擎按照路由协议给出的路由来进行转发操作。

5. IP 地址短缺问题

所谓 IP 地址，就是给每一台连接在 Internet 上的主机分配一个唯一的 32 位地址。IP 地址是由 Internet Assigned Numbers Authority(IANA)组织统一分配的，以保证在 Internet 上没有重复的 IP 地址。

IP 地址由网络号码和主机号码两部分组成。为了便于对 IP 地址进行管理，同时考虑到网络的差异很大，有的网络拥有很多台主机，有的网络上的主机很少，因此，Internet 的 IP 地址分成为五类，即 A～E 类，其中能被使用的是 A，B，C 三类。

A 类 IP 地址的网络号码数不多，目前几乎没有多余的可供分配，现在能够申请到的 IP 地址只有 B 类和 C 类两种。当某个单位申请到 IP 地址时，实际上只是拿到了一个网络号码 net-id。各个主机号码 host-id 由该单位自行分配，只要做到在该单位管辖的范围内无重复的主机号码即可。

由于当初没有预计到计算机会普及得如此之快，各种局域网和局域网上的主机数目急剧增长；另外，由于申请 IP 地址的时候申请的是"网络号码"，在使用时也有很大的浪费。例如，某个单位申请到了一个 B 类地址，但该单位只有 1 万台主机，于是在一个 B 类地址中的其余 5 万 5 千多个主机号码就白白浪费了，因为其他单位的主机无法使用这些号码。地址转换技术就是解决地址短缺问题的主要技术手段。

6. 公有地址和私有地址

Internet 是连接了许多局域网的网络，它可以连接各种不同类型的局域网。局域网的类型很多，本书讨论的都是使用 TCP/IP 协议连接的局域网，如果局域网采用 TCP/IP 协议连接，网中的每台机器都必须拥有一个 IP 地址。为了使局域网的 IP 地址可以被局域网自己规划，IANA 组织在 A，B，C 类 IP 地址中各选出一个网段作为"私有地址"，供各个局域网按照需要自由分配。

私有地址是指内部网络(局域网内部)的主机地址，而公有地址是局域网的外部地址(在 Internet 上的全球唯一的 IP 地址)。IANA 规定以下三个网络地址保留用作私有地址：

```
10.0.0.0～10.255.255.255
172.16.0.0～172.31.255.255
192.168.0.0～192.168.255.255
```

也就是说，这三个网络的地址不会在 Internet 上被分配，但可以在一个企业(局域网)内部使用，各个企业根据可预见的主机数量的多少，来选择合适的网络地址。不同企业的内部网络地址可以相同。如果一个公司选择其他网段作为内部网络地址，有可能引起路由表混乱。

很明显，私有地址是不会在 Internet 上看见的。在 Internet 上可见的 IP 地址称为公有地址，使用私有地址转换的主机是不能直接访问 Internet 的；同样地，在 Internet 上不

可能访问到使用私有地址的主机。

7. 地址转换的优点和缺点

使用地址转换技术主要有以下几个优点：

① 地址转换可以使内部网络用户方便地访问 Internet。

② 地址转换可以使内部局域网的许多主机共享一个 IP 地址上网，大大节约了合法的 IP 地址。

③ 地址转换可以屏蔽内部网络用户，提高内部网络的安全性。

④ 地址转换同样可以提供给外部网络 WWW，FTP，Telnet 等服务。

⑤ 地址转换技术可以使内部局域网的 IP 地址分配容易维护，不会因为合法地址转换的缺乏而不容易合理分配内部局域网的 IP 地址，并且当外部有变化的时候，不需要改动内部局域网内部的配置。

地址转换技术主要有以下几个缺点：

① 地址转换对于报文内容中含有有用的地址信息的情况需要做特殊处理，这种情况的代表协议是 FTP。

② 地址转换不能处理 IP 报头加密的情况。

③ 地址转换由于隐藏了内部主机地址，有时会使网络调试变得复杂。

8. TCP/UDP 端口 NAT 映射

如果 ISP 提供的合法 IP 地址的数量较多，自然可以采用静态地址转换+端口复用动态地址转换的方式得以完美实现内外地址的转换。但如果 ISP 只提供 4 个 IP 地址，其中 2 个作为网络号和广播地址而不可使用，1 个 IP 地址要用于路由器定义默认网关，那么只剩下 1 个 IP 地址可用。当然，也可以利用仅存的这个 IP 地址采用端口复用地址转换技术，实现整个局域网的 Internet 接入。但是由于服务器也采用动态端口，因此，Internet 中的计算机将无法访问到网络内部的服务器。有没有好的解决方案呢？这就是 TCP/UDP 端口 NAT 映射。

我们知道，不同应用程序使用的 TCP/UDP 端口是不同的，比如，Web 服务使用 80，FTP 服务使用 21，SMTP 服务使用 25，POP3 服务使用 110。因此，可以将不同的 TCP 端口绑定至不同的内部 IP 地址，从而只使用一个合法的 IP 地址，即可在允许内部所有服务器被 Internet 访问的同时，实现内部所有主机对 Internet 的访问。

9. 利用地址转换实现负载均衡

随着访问量的上升，当一台服务器难以胜任时，必须采用负载均衡技术，将大量的访问合理地分配至多台服务器。实现负载均衡的手段有许多种，比如采用服务器群集负载均衡、交换机负载均衡、DNS 解析负载均衡等；也可以通过地址转换方式实现服务器的负载均衡。事实上，这些负载均衡的实现大多采用轮询方式实现，使每台服务器都拥有平等的被访问机会。

思考训练(评估)

1. 思考与提高

(1) 路由的基本原理是什么?
(2) IP 地址中的私有地址是什么?
(3) NAT 的作用是什么?
(4) 在 NAT 中有哪 4 种地址?
(5) 最常用的网络地址转换模式有哪几种?

2. 实训

(1) 掌握相应计算机和路由器的连接、启动路由器、初始化路由器、登录路由器的基本操作,熟悉各种编辑命令和帮助命令的使用。

(2) 配置静态路由协议。

有两台路由器 Route A 和 Route B。Route A 的 S0 口与 Route B 的 S1 口直连。为两个端口分别配置 IP 地址。同时,Route A 还连接了一个 172.16.1.0 网络,Route B 上连接了一个 192.167.1.0 网络,在路由器上分别配置网络。请配置静态路由,使网络间能够通信。

(3) 配置 OSPF 协议。网络拓扑结构如图 3-12 所示。注意,路由器之间采用串行电缆连接,请根据图示结构构建 OSPF 路由协议。

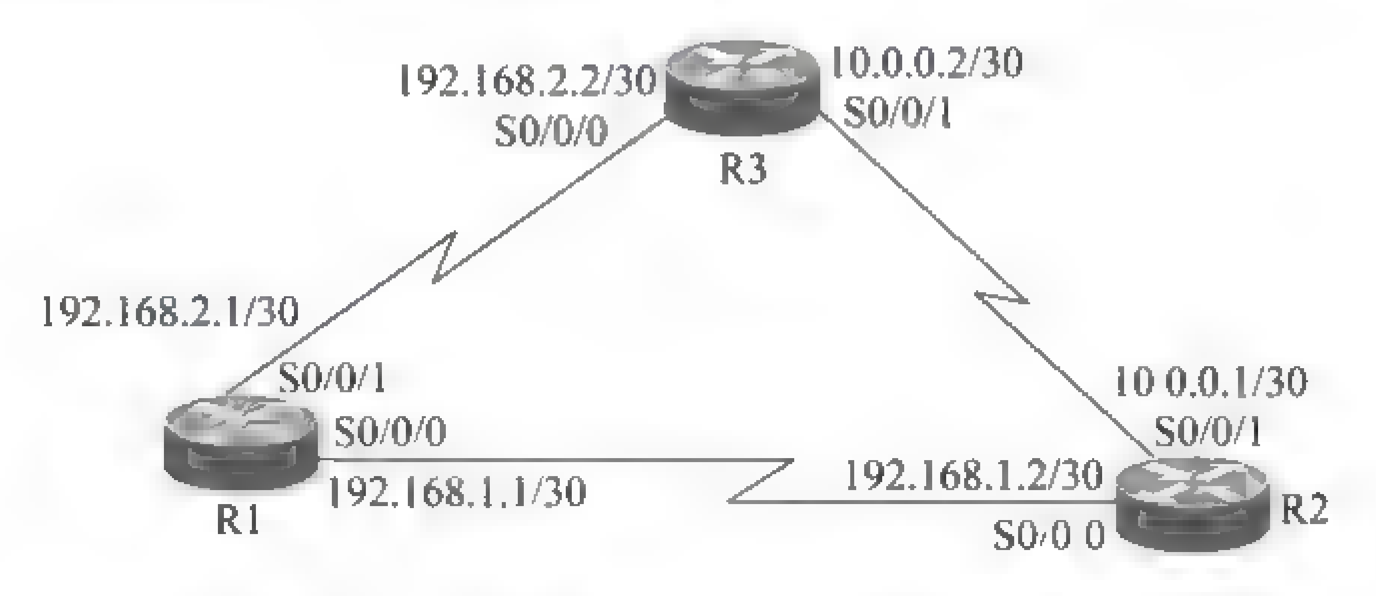


图 3-12　OSPF 协议配置的网络拓扑结构

(4) 某公司的网络由两台路由器 RTA 和 RTC 组成。路由器 RTA 是连接 ISP 的边界路由器,ISP 只分配了一个子网 192.168.1.32/27 给该公司的网络。因为这个子网只允许有 30 台主机,所以该公司决定在网络内部运行 NAT,使公司内部的几百台主机共享这 30 个全局地址。除了配置 NAT 复用以外,公司还要求实施 TCP 负载均衡,使外部来的 Web 请求被均衡在两台不同的内部 Web 服务器上。公司内部的网络 IP 地址分配为 10.0.0.0/8 网段。

NAT 网络拓扑结构如图 3-13 所示,按照拓扑图组建网络。根据拓扑结构的要求,给路由器各端口配置 IP 地址、子网掩码、时钟(DCE 端),并将各端口启动,还要配置主机 A 和主机 B 的 IP 地址、子网掩码、网关等信息。上述信息配置完毕后,用 ping 命令测试直接相连的设备之间是否能够通信。配置 RTA 作为一台 NAT 服务器,RTA 将把该公

司的内部地址(10.0.0.0/8)转换为 ISP 所分配的地址(192.168.1.32/27)。

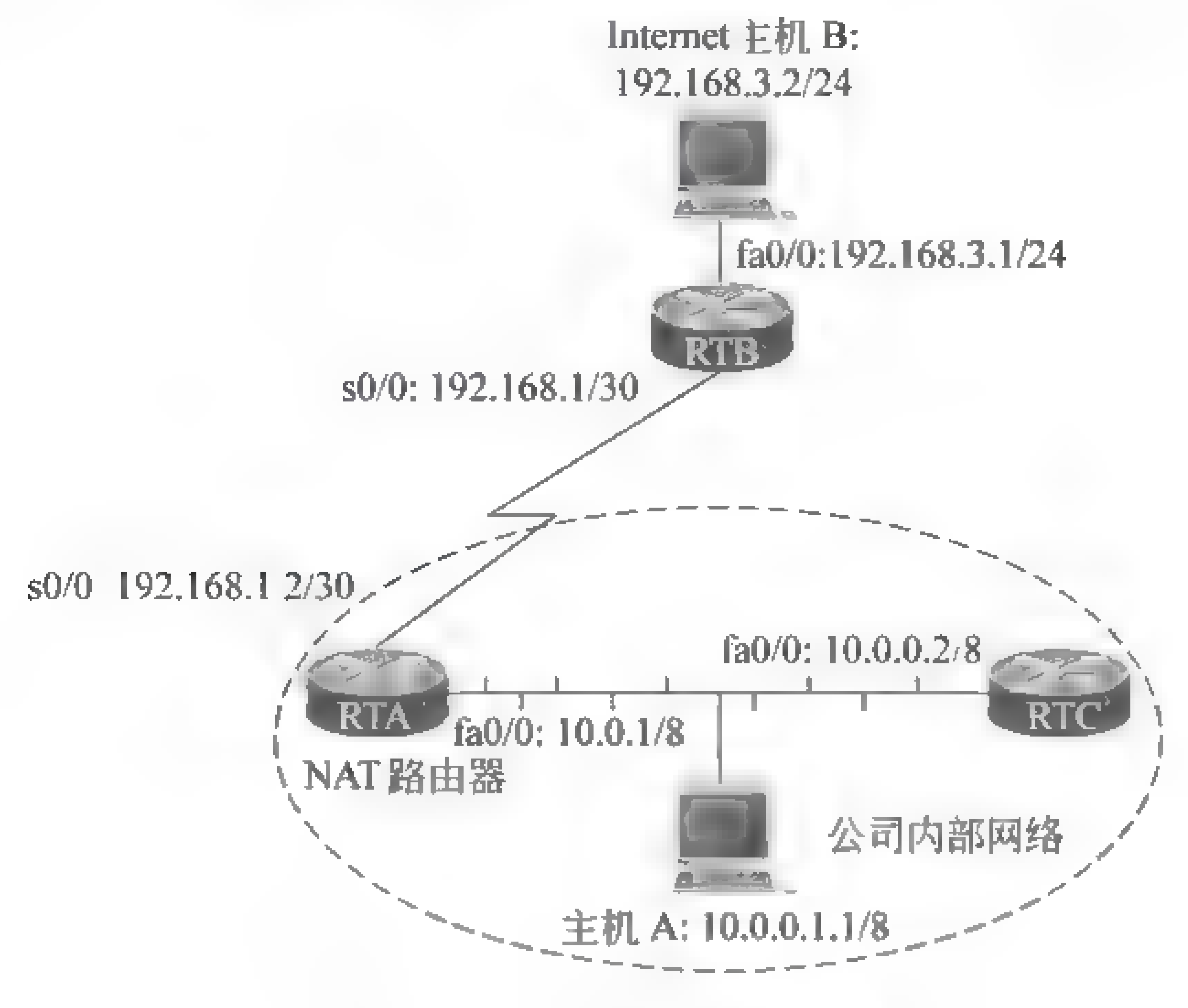


图 3-13 NAT 网络拓扑结构

学习情境4　网络安全配置

任务情境(资讯)

ThreeFour Software公司在网络中应用了STP协议之后,既解决了交换机之间的环路,又提供了冗余备份的链路,网络可靠性得到了很大改善。现在网络面临安全问题。为了防止非法用户使用公司的局域网资源,李四希望能对所有接入到公司以太网交换机的用户都进行验证,验明其合法身份后再使用网络资源。

随着网络复杂程度的增加,出于安全方面的考虑,李四希望能够在公司网络中实现一定的访问控制,比如将研发部和市场部的网络隔离开,分支机构的网络只能访问总部的某些特定服务。要实现上述功能,需要用到防火墙技术。

公司有防火墙,在机房对防火墙进行初始配置后,可以通过Web方式对防火墙进行远程配置和管理。公司在全国各地都有办事机构,需要访问公司内部的服务器资源,而这些服务器资源出于安全性考虑不直接在公网上开放,因此必须通过建立VPN隧道,再获得访问内部资源的权利。

任务分析(决策)

在上述情境中,我们会遇到5个核心问题,即网络安全设备、802.1认证、ACL访问控制列表、防火墙和虚拟专用网络(VPN)。为了完成以上任务,先介绍以下理论。

1. 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护,不因偶然的或者恶意的原因而遭受到破坏、更改、泄漏,系统可以连续、可靠、正常地运行,网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说,凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全的具体含义会随着"角度"的变化而变化。比如,从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。

2. 802.1认证

802.1x协议起源于802.11协议,后者是IEEE的无线局域网协议,制定802.1x协

议的初衷是为了解决无线局域网用户的接入认证问题。IEEE 802 LAN 协议定义的局域网并不提供接入认证,只要用户能接入局域网控制设备(如 LAN Switch),就可以访问局域网中的设备或资源。这在早期企业网有线 LAN 应用环境下并不存在明显的安全隐患。但是随着移动办公及驻地网运营等应用的大规模发展,服务提供者需要对用户的接入进行控制和配置。尤其是 WLAN 的应用和 LAN 接入在电信网上大规模开展,有必要对端口加以控制,以实现用户级的接入控制。802.1x 就是 IEEE 为了解决基于端口的接入控制(Port-Based Network Access Control)而定义的一个标准。

IEEE 802.1x 是根据用户 ID 或设备,对网络客户端(或端口)进行鉴权的标准。该流程称为“端口级别的鉴权”。它采用 RADIUS(远程认证拨号用户服务)方法,并将其划分为三个不同的小组:请求方、认证方和授权服务器。

820.1x 标准应用于试图连接到端口或其他设备(如 Cisco Catalyst 交换机或 Cisco Aironet 系列接入点)(认证方)的终端设备和用户(请求方)。认证和授权都通过鉴权服务器(如 Cisco Secure ACS)后端通信实现。IEEE 802.1x 提供自动用户身份识别,集中进行鉴权、密钥管理和 LAN 连接配置。整个 802.1x 的实现涉及设计三个部分,即请求者系统、认证系统和认证服务器系统。

3. ACL 访问控制列表

访问控制列表(ACL,Access Control List)是路由器和交换机接口的指令列表,用来控制端口进出的数据包。ACL 适用于所有的路由协议,如 IP、IPX、AppleTalk 等。这张表中包含了匹配关系、条件和查询语句,表只是一个框架结构,其目的是为了对某种访问进行控制。

信息点间通信及内、外网络的通信都是企业网络中必不可少的业务需求,但是为了保证内网的安全性,需要通过安全策略来保障非授权用户只能访问特定的网络资源,达到对访问进行控制的目的。简而言之,ACL 是过滤网络中的流量,控制访问的一种网络技术手段。

ACL 的定义也是基于每一种协议的。如果路由器接口配置成为支持三种协议(IP,AppleTalk 以及 IPX)的情况,那么,用户必须定义三种 ACL 来分别控制这三种协议的数据包。

4. ACL 的作用

ACL 可以限制网络流量,提高网络性能。例如,ACL 可以根据数据包的协议,指定数据包的优先级。

ACL 提供对通信流量的控制。例如,ACL 可以限定或简化路由更新信息的长度,从而限制通过路由器某一网段的通信流量。

ACL 是提供网络安全访问的基本手段。ACL 允许主机 A 访问人力资源网络,而拒绝主机 B 访问。

ACL 可以在路由器端口处决定哪种类型的通信流量被转发或被阻塞。例如,用户可以允许 E mail 通信流量被路由,拒绝所有的 Telnet 通信流量。例如,某部门要求只能使

用 WWW 这个功能，就可以通过 ACL 实现；又如，为了某部门的保密性，不允许其访问外网，也不允许外网访问它，可以通过 ACL 实现。

ACL 的执行流程如下：如果一个数据包的报头跟 ACL 中某个条件判断语句相匹配，那么后面的语句就将被忽略，不再进行检查。数据包只有在跟第一个判断条件不匹配时，它才被交给 ACL 中的下一条条件判断语句进行比较。如果匹配（假设为允许发送），则不管是第一条还是最后一条语句，数据都会立即发送到目的接口。如果所有的 ACL 判断语句都检测完毕，仍没有匹配的语句出口，则该数据包将视为被拒绝而被丢弃。

注意：ACL 不能对本路由器产生的数据包进行控制。

5. 防火墙

所谓防火墙，指的是一个由软件和硬件设备组合而成，在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障，是一种获取安全性方法的形象说法。它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），保护内部网免受非法用户的侵入。防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。

防火墙是一个位于计算机和它所连接的网络之间的软件或硬件（其中，硬件防火墙用得较少，国防部以及大型机房等地才用，因为它价格昂贵）。该计算机流入、流出的所有网络通信均要经过此防火墙。

防火墙对流经它的网络通信进行扫描，过滤掉一些攻击，以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口，禁止特定端口的流出通信，封锁“特洛伊木马”。最后，它可以禁止来自特殊站点的访问，防止来自不明入侵者的所有通信。

6. 什么是 VPN

VPN 的英文全称是“Virtual Private Network”，即虚拟专用网络，可以把它理解成虚拟出来的企业内部专线。它可以通过特殊的加密的通信协议，在连接到 Internet 上的位于不同地方的两个或多个企业内部网之间建立一条专有的通信线路，就像架设了一条专线一样，但并不需要真正敷设光缆之类的物理线路。这就好比去电信局申请专线，但是不用付敷设线路的费用，也不用购买路由器等硬件设备。VPN 原是路由器的重要技术之一，目前在交换机、防火墙设备或 Windows 2000 软件里也支持 VPN 功能。总之，VPN 的核心就是利用公共网络建立虚拟私有网。

虚拟专用网（VPN）被定义为通过公用网络（通常是 Internet）建立一个临时的、安全的连接，它是一条穿过混乱的公用网络的安全、稳定的隧道。虚拟专用网是对企业内部网的扩展。虚拟专用网可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输。虚拟专用网可用于不断增长的移动用户的全球 Internet 接入，实现安全连接；可用于实现企业网站之间安全通信的虚拟专用线路，用于经济、有效地连接到商业伙伴和用户的安全外联网。

任务设计(计划)

在简单了解了用于网络安全的基本方法和概念后,下面根据 ThreeFour Software 公司的具体情况,分4个任务来解决问题。

任务 4.1　认识基于设备的网络安全

任务 4.2　配置 ACL(访问控制列表)

任务 4.3　设置防火墙

任务 4.4　建立外部安全数据通道——VPN

任务实施(实施)

任务 4.1　认识基于设备的网络安全

情境回顾:为了维护好公司的网络并保证网络安全,公司购买了相应的网络安全产品,王五是公司的网络管理员,负责网络中心设备的管理工作。公司内部安装了网络安全产品,王五需要配置它,使网络更加安全。

首先要熟悉网络安全设备防火墙、IDS、VPN 设备。

4.1.1　防火墙的应用

1. 防火墙是网络安全的屏障

防火墙(作为阻塞点、控制点)能极大地提高内部网络的安全性,并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙,所以网络环境变得更安全。如防火墙可以禁止不安全的 NFS 协议进出受保护网络,外部的攻击者就不可能利用这些脆弱的协议来攻击内部网络。防火墙同时可以保护网络免受基于路由的攻击,如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

2. 防火墙可以强化网络安全策略

通过以防火墙为中心的安全方案配置,能将所有安全软件(如口令、加密、身份认证、审计等)配置在防火墙上。与将网络安全问题分散到各个主机上相比,防火墙的集中安全管理更经济。例如在网络访问时,一次一密口令系统和其他的身份认证系统完全不必分散在各个主机上,而集中在防火墙上。

3. 对网络存取和访问进行监控、审计

如果所有访问都经过防火墙,那么,防火墙就能记录下这些访问并作出日志记录,同时提供网络使用情况的统计数据。当发生可疑动作时,防火墙能适当报警,并提供网络是

否受到监测和攻击的详细信息。另外，收集网络的使用和误用情况也是非常重要的。首先可以清楚防火墙是否能够抵挡攻击者的探测和攻击，并且清楚防火墙的控制是否充足。网络使用情况统计对网络需求分析和威胁分析而言也是非常重要的。

4.1.2 IDS的应用

IDS是英文"Intrusion Detection Systems"的缩写，即入侵检测系统。专业上讲就是依照一定的安全策略，对网络、系统的运行状况进行监视，尽可能发现各种攻击企图、攻击行为或者攻击结果，以保证网络系统资源的机密性、完整性和可用性。

可以做一个形象的比喻：假如防火墙是一幢大楼的门锁，IDS就是这幢大楼里的监视系统。一旦小偷爬窗进入大楼，或内部人员有越界行为，只有实时监视系统才能发现情况并发出警告。

不同于防火墙，IDS入侵检测系统是一个监听设备，没有跨接在任何链路上，无须网络流量流经它便可以工作。因此对IDS的部署，唯一的要求是：IDS应当挂接在所有所关注流量都必须流经的链路上。在这里，"所关注流量"指的是来自高危网络区域的访问流量和需要进行统计、监视的网络报文。在如今的网络拓扑中，已经很难找到以前的HUB式的共享介质冲突域的网络，绝大部分网络区域都已经全面升级到交换式网络结构。因此，IDS在交换式网络中的位置一般选择在尽可能靠近攻击源或尽可能靠近受保护资源的地方，通常是服务器区域的交换机上、Internet接入路由器之后的第一台交换机上或是重点保护网段的局域网交换机上。

防火墙和IDS可以分开操作。IDS是监控系统，可以选择合适的或是符合需求的，若发现规则或监控不完善，可以更改设置及规则，或是重新设置。

早期的IDS仅仅是一个监听系统。这里，可以把"监听"理解成"窃听"。基于目前的局域网工作方式，IDS可以将用户对位于与IDS在同一交换机/HUB服务器的访问、操作全部记录下来供分析使用，跟常用的Windows操作系统的事件查看器类似。后来，由于IDS的记录太多，新一代IDS将记录的数据进行分析，仅列出有危险的一部分记录，跟Windows所用的策略审核很类似。目前的IDS增加了分析应用层数据的功能，配合防火墙进行联动，可分析出有敌意的地址并阻止其访问。

如理论与实际的区别一样，IDS虽然具有上面所说的优点，但在实际使用中，大多数入侵检测都采用pass by的方式来侦听网络上的数据流，这就限制了IDS本身的阻断功能。IDS只有靠发阻断数据包来阻断当前行为，并且IDS的阻断范围很小，只能阻断建立在TCP基础之上的行为，如Telnet、FTP、HTTP等，而对于建立在UDP基础之上的行为就无能为力了。因为防火墙的策略都是事先设置好的，无法动态设置，缺少针对攻击的必要的灵活性，不能更好地保护网络的安全，所以IDS与防火墙联动能更有效地阻断所发生的攻击事件，使网络隐患降至较低的限度。

任务 4.2 配置 ACL（访问控制列表）

网络管理者需要了解怎样控制有害的网络访问，允许恰当的网络访问。尽管有多种措施，如设置密码、添加物理上的安全设备等，这些方法当然是有用的，但是它们缺少网络管理者所期望的灵活的基本数据流过滤能力和特定的控制能力。

路由器提供了基本的数据流过滤能力，如使用访问控制列表（ACL，Access Control List），可以阻止 Internet 数据流。ACL 是一系列允许或拒绝访问的指令的集合，这些指令将运用到网络地址或者上层协议中。本节将介绍使用标准的和扩展的 ACL 作为控制网络数据流的方式和网络安全的解决方案。本节还将介绍使用 ACL 的一般规则、提示和建议，以及创建 ACL 所需的命令和配置。最后，本节提供了使用标准和扩展 ACL 的实例，介绍了如何将 ACL 绑定到路由器的接口。

4.2.1 ACL 概述

1. 什么是 ACL

ACL 是运用到路由器接口的指令列表。这些指令告诉路由器接收哪些数据包，拒绝哪些数据包。接收或者拒绝根据一定的规则进行，如源地址、目标地址、端口号等。ACL 使得用户能够管理数据流，检测特定的数据包。路由器将根据 ACL 中指定的条件，对经过路由器端口的数据包进行检查。

ACL 可以基于所有的路由协议，如 IP 和 IPX，对经过路由器的数据包进行过滤。基于 IP 协议的 ACL 称为 IP ACL，基于 IPX 的 ACL 称为 IPX ACL，本节只介绍 IP ACL。另外，ACL 可以配置成控制对网络或者子网的访问。

按照路由器 ACL 在端口过滤网络数据流，决定是否转发或者阻止可路由数据包。路由器根据 ACL 中指定的条件决定转发或者丢弃数据包。这些条件可以是数据包的源地址、目的地址、上层协议或者其他信息。

ACL 应该根据路由器的端口所允许的每个协议来制定，如果需要控制流经某个端口的所有数据流，需要为该端口允许的每一个协议分别创建 ACL（某些协议将 ACL 称为过滤器）。例如，如果端口配置成允许 IP、AppleTalk 和 IPX 协议的数据流，那么需要创建至少三个 ACL。ACL 可以用做控制和过滤流经路由器端口的数据包的工具。

2. ACL 的用途

① 限制网络数据流、增加网络性能。例如，根据不同的协议，ACL 可以指定路由器先处理哪些数据包，这叫做队列管理，使得路由器不去处理不需要的数据包，结果是队列管理限制了网络数据流，减少了网络拥塞。

② 提供数据流控制。例如，ACL 可以限定或者减少路由更新的内容。这些限定用

于限制关于某个特定网络的信息传播到整个网络。

③ 为网络访问提供基本的安全层。ACL 可以允许某个主机访问网络的某一部分，而阻止另一台主机访问网络的这个部分。主机 A 可以访问某个子网，主机 B 禁止访问该子网，假如不在路由器上配置 ACL，所有流经路由器的数据包都允许进入网络的所有部分。

④ 决定转发或者阻止哪些类型的数据流。例如，允许路由 E-mail 的数据流，而阻止 Telnet 的数据流。

4.2.2 ACL 的工作过程

ACL 的工作原理是查看数据包的第三层或者第四层信息。通过读取数据包的这些信息，ACL 按照事先设置好的一套规则来决定如何处理数据包，是将它们转发到目的地，还是丢弃该数据包。ACL 可以说是防火墙的雏形。当然，仅仅对逻辑地址进行安全检查没有多大作用，因为很多黑客攻击都能够隐藏或修改地址，应当把 ACL 与其他安全方式结合起来，才能提高安全性。

1. ACL 的操作过程

若路由器配置了 ACL，要在转发之前将数据发往 ACL 进行验证。如果通过验证，路由器将其转发；如果没有通过验证，路由器将其丢弃。

创建了 ACL 之后，可以将其绑定到路由器的入口或者出口，分别称为入栈 ACL 和出栈 ACL。

(1) 入栈(Inbound)ACL

入栈 ACL 指 ACL 被绑定到路由器某个接口的入口。当在该接口收到数据时，先进行 ACL 检查，只有通过检查，才允许该数据包进入路由器。路由器再查看路由表，然后将数据包转发，否则该数据包在进入路由器之前就被丢弃了。

当数据包进入路由器时，首先检查该接口是否绑定了入栈 ACL。如果绑定了入栈 ACL，入栈 ACL 会对数据包进行检查。如果符合 ACL 的条件，将该数据包送入路由表进行路由转发；如果不符合 ACL 的条件，则丢弃该数据包。

另外，使用入栈 ACL 会大大提高路由器的性能，因为先要检查数据，然后转发，这样，非法数据包在进入路由表之前就被丢弃了，节省了路由表的查找开销。

(2) 出栈(Outbound)ACL

出栈 ACL 指 ACL 被绑定到路由器某个接口的出口。数据包从某个接口进入路由器，经过路由表转发。当转发到绑定了出栈 ACL 的接口时，进行数据包出栈检查。如果通过检查，数据包可以从该接口转发出去；如果没有通过检查，数据包将被丢弃。

当数据包从某个接口进入路由器时，如果进入接口没有绑定入栈 ACL，则通过路由表转发。当决定转发到某个输出接口时，在数据包从输出接口出去之前，会检查该出口是否绑定了出栈 ACL。如果绑定了出栈 ACL，出栈 ACL 会对该数据包进行检查。如果符

合条件，将数据包从该接口转发出去；如果不符合条件，则丢弃该数据包。

也就是说，对于入栈 ACL，“允许”意味着路由器在该接口接收到的数据包进行下一步处理（路由，转发）；“拒绝”意味着丢弃该数据包，并返回 ICMP 信息。对于出栈 ACL，“允许”意味着数据包被发送到输出接口；“拒绝”意味着丢弃该数据包，并返回 ICMP 信息。

2. ACL 的逻辑测试过程

访问控制列表（ACL）是一张由多条命令组成的“表”，这些命令语句规定了一个或多个逻辑条件。命令语句的一般格式是：

条件+满足条件采取的操作

例如，该命令的条件是 IP 地址为 1.1.1.1，如果数据包的 IP 地址恰为 1.1.1.1，则表明条件匹配。条件匹配后，根据命令的操作进行转发或丢弃。

数据包进入 ACL 的测试过程中，会按照 ACL 中命令语句的顺序从上至下检查。

① 如果数据包与 ACL 中的某条语句匹配，则列表中的其他语句被忽略。注意，“匹配”是指数据包满足该命令的条件。

② 如果数据包与某个命令不匹配，则继续检查 ACL 下一条命令语句，直到匹配为止。

③ 如果到达 ACL 的最后一条命令仍不匹配，数据包会被丢弃。这是因为 ACL 中隐含了一条命令语句：拒绝所有。该语句的条件是“所有”操作是“拒绝”。当数据包到达最后这条隐含语句时，当然会满足该语句的条件（所有），因此被拒绝了。

例如，某个 ACL 要求只允许主机 192.168.1.1 和网络 172.16.0.0 的数据包通过，可以包含如下命令。

第一条命令：“条件”为 IP 地址 192.168.1.1；“操作”为允许。

第二条命令：“条件”为网络地址 172.16.0.0；“操作”为允许。

当某个数据包的地址是 192.168.1.1 时，数据包进入 ACL 接受第一条命令的检查，条件匹配，允许通过，并且退出 ACL 的检查，不会接受第二条命令的检查。

当某个数据包的地址是 1.1.1.1 时，数据包进入 ACL，接受第一条命令的检查，条件不匹配；接受第二条命令的检查，条件仍不匹配；接受隐含命令的检查，条件匹配，拒绝。

注意：

① 因为 ACL 包含了一条隐含语句“拒绝所有”，因此使用 ACL 要小心，至少 ACL 中要有一条允许语句，否则所有数据包都会被 ACL 拒绝。

② ACL 命令的配置顺序是很重要的。当路由器决定是否转发或者阻止数据包的时候，Cisco 的 IOS 软件按照 ACL 中指令的顺序依次检查数据包是否是某一个指令条件，所以应该把限制最严格的语句放在 ACL 的顶端，以提高性能。

③ 当检测到某个命令条件满足的时候，就不再检测后面的指令条件。

④ 应该先建立 ACL，再将其绑定到入口或者出口。

⑤ ACL 只能过滤通过路由器的数据流量，不能过滤路由器本身产生的数据流量。

4.2.3 ACL 分类

根据对数据包的检查过程，有两类 ACL：标准 ACL(Standard)和扩展 ACL(Extended)。标准 ACL 检查数据包的源地址，然后决定允许还是拒绝转发该数据包。扩展 ACL 检查数据包的源地址、目的地址、特定协议、端口号码以及其他参数。扩展 ACL 使用更灵活。

1. 标准 ACL

标准 ACL 通过查看数据包的源逻辑地址来判断取舍，即只检查数据包的第三层信息，而不检查其他信息，因此它不能对数据包进行更精确的检验。例如，图 4-1 所示是一个标准 ACL，可以在路由器的 E0 口上绑定出栈 ACL，禁止网络 172.16.0.0 访问网络 10.0.0.0 而允许 192.168.1.0 访问。



图 4-1 标准 ACL　　　　图 4-2 扩展 ACL

2. 扩展 ACL

扩展 ACL 不仅查看数据包的源地址，而且查看数据包的目的地址、端口号、协议等信息，即既查看第三层信息，又查看第四层信息。因此，扩展 ACL 可以进行更加灵活的检验。例如，它允许某台主机通过 FTP(端口号 21)协议访问某个网络，而不允许它通过 Telnet(端口号 23)访问，如图 4-2 所示。

在图 4-2 中，可以在路由器的 E2 接口绑定出栈 ACL，允许主机 172.16.1.1 通过 FTP 访问主机 192.168.1.1，而不允许通过 Telnet 访问。

4.2.4 ACL 配置

不管是标准 ACL 还是扩展 ACL，它们的配置步骤都遵循两个过程：创建 ACL 和将 ACL 绑定到某个接口。

1. 创建 ACL

配置 ACL 的第一步是先创建 ACL。我们知道，ACL 是一个包含着一条或多条命令的“表”，创建 ACL 其实就是向某个 ACL 填写命令的过程。

命令的一般格式是：

ACL编号+操作+条件

另外，配置ACL的时候需要为每一个协议的ACL指定一个唯一的数字，用于标识这个ACL。这个数字必须在有效的范围之内。

为每一个协议的ACL指定的数字范围如表4-1所示。创建ACL的通用命令如表4-2所示。

表4-1 ACL的编号范围

IP ACL	编号范围	IP ACL	编号范围
标准ACL	1～99	标准ACL	800～899
扩展ACL	100～199	扩展ACL	900～999

表4-2 创建ACL的通用命令

命令	说明
Router(config)# access-list ACL编号 [permit|deny] 测试条件	创建某个ACL，并向其中添加一条命令语句
Router(config)# no access-list ACL编号	删除某个ACL

说明：

① 可以向一个ACL写入多条语句。

② ACL的配置命令比较繁琐，尤其是需要向一个ACL添加多条命令语句时，使用文本文件事先将命令编辑好，再复制、粘贴到IOS中是一个不错的办法。

③ 使用"no access-list 编号"删除整个ACL。注意，在标准和扩展ACL中，不能够删除ACL中的某一条命令语句，只能一次删除整个ACL。

2. 将ACL绑定到某个接口

创建了ACL，就可以将它绑定到路由器的某个接口。注意，一定要先创建再绑定。表4-3所示是绑定的通用命令。

表4-3 绑定ACL的通用命令

命令	说明
Router(config-if)# protocol access-group ACL编号[in|out]	将某个ACL绑定到路由器的某个接口上。参数protocol指明了是基于什么协议的ACL，常用的有IP和IPX；参数in/out指明是绑定到入口还是出口

4.2.5 通配符掩码

ACL通过测试进入的数据包是否符合某个条件来决定是允许还是拒绝发送，那么，需要某种方法来识别给定的IP地址是否匹配规定的条件。通配符掩码(Wildcard Bits)

用于检测条件是否匹配。

路由器使用通配符掩码与源或目标地址一起来分辨匹配的地址范围。正如子网掩码告诉路由器IP地址的哪一位属于网络号一样，通配符掩码告诉路由器如何判断是否匹配，它需要检查IP地址中的多少位。这个地址掩码对(由地址和掩码组成的一对数字)只使用两个32位号码来确定IP地址的范围，这是十分方便的。因为如果没有掩码的话，用户不得不对每个匹配的IP客户地址加入单独的访问列表语句，这将造成路由器大量额外的处理过程，所以地址掩码对相当有用。

与子网掩码类似，通配符掩码是由0，1二进制数组成的32位数字，分成4段。32位中的每一位正好和IP地址的相应位对应，如图4-3所示。

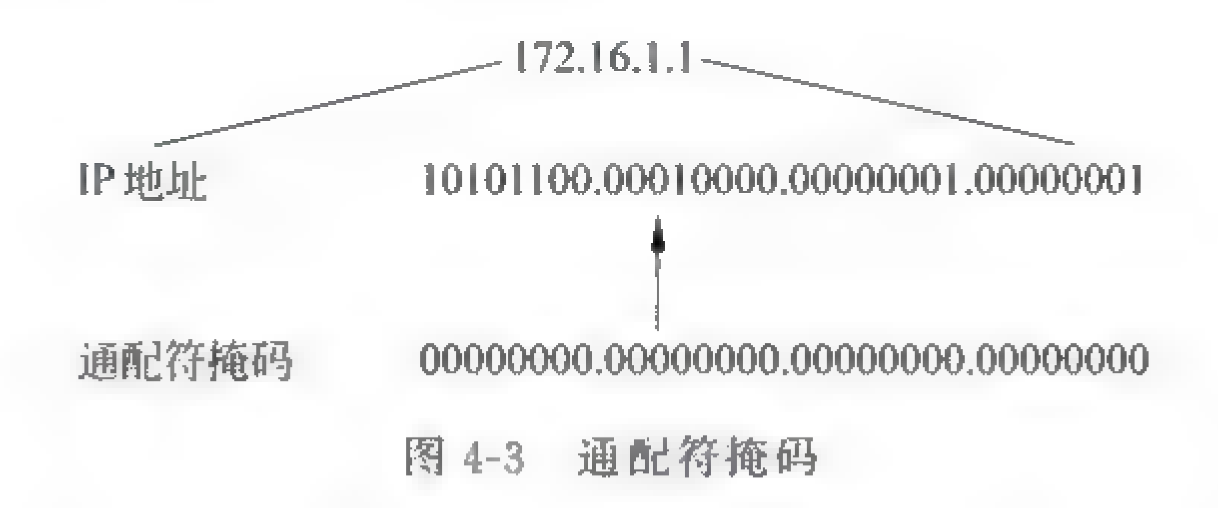


图4-3　通配符掩码

可以配置通配符掩码来决定检查IP地址的哪一位，忽略哪一位，检查规则如下：

① 通配符掩码为1的那一位意味着忽略该位所对应的IP地址的那一位。

② 通配符掩码为0的那一位意味着检查该位所对应的IP地址的那一位。

例如，如图4-4所示，通配符掩码是0.0.0.255，意味着检查前三个8位组的最后一个8位。该通配符掩码与IP地址172.16.1.1组合形成地址掩码时会产一个条件：所有IP地址的前三组8位是172.16.1的主机(即网络ID是172.16.1.0的主机)。

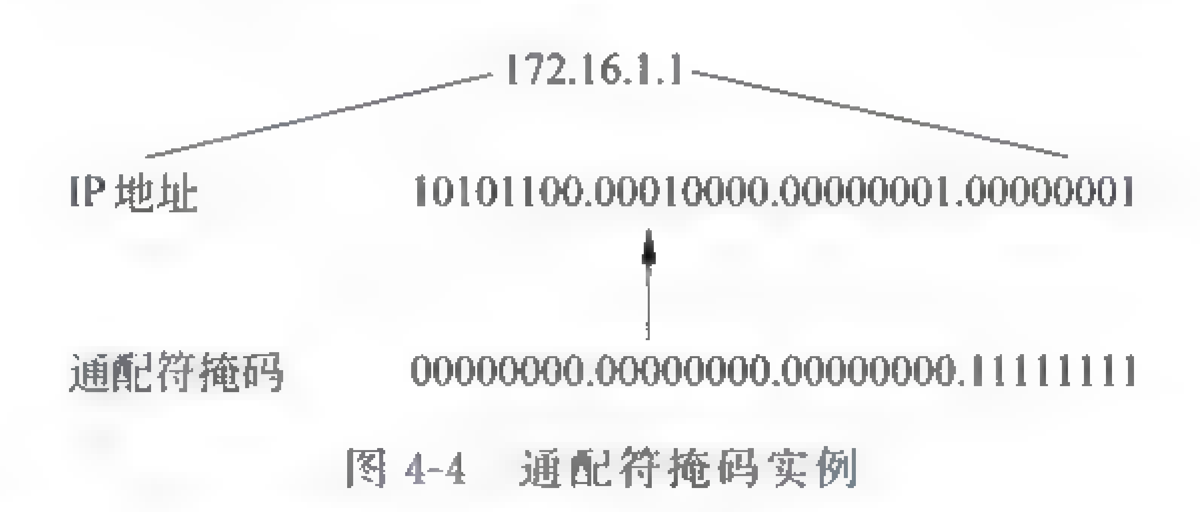


图4-4　通配符掩码实例

当然，刚才的例子是非常简单的一种情况，如果IP地址172.16.144.0和通配符掩码0.0.15.255组成地址掩码对，检测的条件会是怎样的呢？下面来分析一下。

如图4-5所示，符合条件的网络是172.16.145.0～172.16.159.0。可以看出，在上面的IP地址中，前两个8位是172.16，第3个8位的前4位是1001，满足了条件，后12位可以是任意数字，因为对应后12位的掩码都是1。由此可以看出，使用通配符掩码不仅可以检查某个主机、某个网络，还可以检查某一些网络，因此灵活地配置通配符掩码可以满足不同的网络要求。

	172.16.144.0
IP 地址	172.16.10010000.0
通配符掩码	0.0.00001111.255
可用的网络	172.16.10010001.0=172.16.145.0
	172.16.10010002.0=172.16.146.0
	⋮
	172.16.10011111.0=172.16.159.0

图 4-5　地址掩码对

通配符掩码与子网掩码是很容易混淆的两个概念，尽管都是 32 位的，但是通配符掩码与 IP 子网掩码的工作原理不同。在子网掩码中，0 或者 1 决定了相应主机的 IP 地址是网络位、子网位，还是主机位；在通配符掩码中，相应位 0 或者 1 决定 ACL 是否检查或者忽略 IP 地址中的相应位。

1. any 命令

与十进制数表示的二进制通配符掩码位打交道是很枯燥的，某些通配符掩码可以使用缩写形式替代。这些缩写形式减少了在配置地址、检查条件时的输入量。例如，假如想使任何目标地址都被允许，为了检查地址，需要输入 0.0.0.0。要使 ACL 忽略任意值，通配符掩码为 255.255.255.255，可以使用缩写形式指定相同的测试条件。例如，替代下面的地址掩码对：

```
0.0.0.0. 255.255.255.255
```

可以使用

```
any
```

2. host 命令

当想匹配 IP 地址中所有的位时，Cisco IOS 允许使用另一个 ACL 通配符掩码的缩写。假如想指定一个特定的 IP 地址在 ACL 的检查中被允许。为了指明这个主机地址，输入整个地址(如 171.30.16.29)。然后，为了指明 ACL，将检查地址中的所有位以及相应的通配符掩码的各位设置成 0(即 0.0.0.0)，可以使用缩写形式。在这个例子中，为了替换 171.30.16.29 0.0.0.0，可以在地址前使用 host。

例如，为了替换地址掩码对 171.30.16.29 0.0.0.0，可使用 host 171.30.16.29。

4.2.6　标准 ACL 的配置

如果想允许/禁止来自于某个网络的所有数据流，或者禁止某一套协议的数据流，可以使用标准 ACL。标准 ACL 检查可路由的数据包的源地址，即根据源地址中的网络、子网和主机地址，判断允许或者拒绝来自于整套协议的数据包。例如，对于来自 E0 端口的数据包，将检查它的源地址和协议。如果被允许，将输出到 S0 端口；如果被禁止，数据包

将被丢弃。

标准 ACL 的配置过程分为两步：创建 ACL 和绑定 ACL，其配置命令如表 4-4 所示。

表 4-4　标准 ACL 的配置

命　　令	说　　明
Router(config) # access-list ACL 编号 [permit|deny]源地址　通配符掩码	创建标准 ACL。注意，ACL 编号范围必须是 1～99，默认通配符掩码是 0.0.0.0
Router(config-if) # ip access-group ACL 编号[in|out]	将一个已存在的 ACL 绑定到某个接口上，参数 in out 指明是入栈 ACL 还是出栈 ACL。默认为出栈 ACL
Router # show access-list[ACL 编号]	查看已经存在的 ACL 包含的命令语句，如果不指定 ACL 编号，则显示所有的 ACL
Router # show ip interface 接口标识	查看是否为某个接口绑定了 ACL

注意：对于任一端口的各个协议的每一个方向，只允许存在一个 ACL。

例如：

```
Router(config)#access-list 1 permit 191.5.34.0 0.0.0.255
Router(config)#access-list 1 permit 128.88.0.0 0.0.255.255
Router(config)#access-list 1 permit 36.0.0.0 0.255.255.255
Router(config)#interface E0
Router(config-if)#ip access-group 1 out
Router#show access-list 1
```

输出结果如下：

```
Standard IP access list 1
permit 191.5.34.0
permit 128.88.0.0
permit 36.0.0.0
```

在这个例子中，通配符掩码运用到网络地址部分。对于任何源地址，如果与 ACL 指令不匹配，都将被拒绝。

为了使指定大量的单个地址更容易，如果通配符掩码是全 0，可以忽略通配符掩码，这样，下面的三条配置命令具有相同的效果：

```
access-list 2 permit 36.48.0.3
access-list 2 permit 36.48.0.3 0.0.0.0
access-list 2 permit host 36.48.0.3
```

例 4-1　指定特定网络。

只允许来自网络 171.16.0.0 的数据包被转发，其余的数据包都将被阻止，如图 4-6 所示。

(1) 创建标准 ACL，命令如下：

```
Router(config)#access list 1 permit 171.16.0.0 0.0.255.255
```

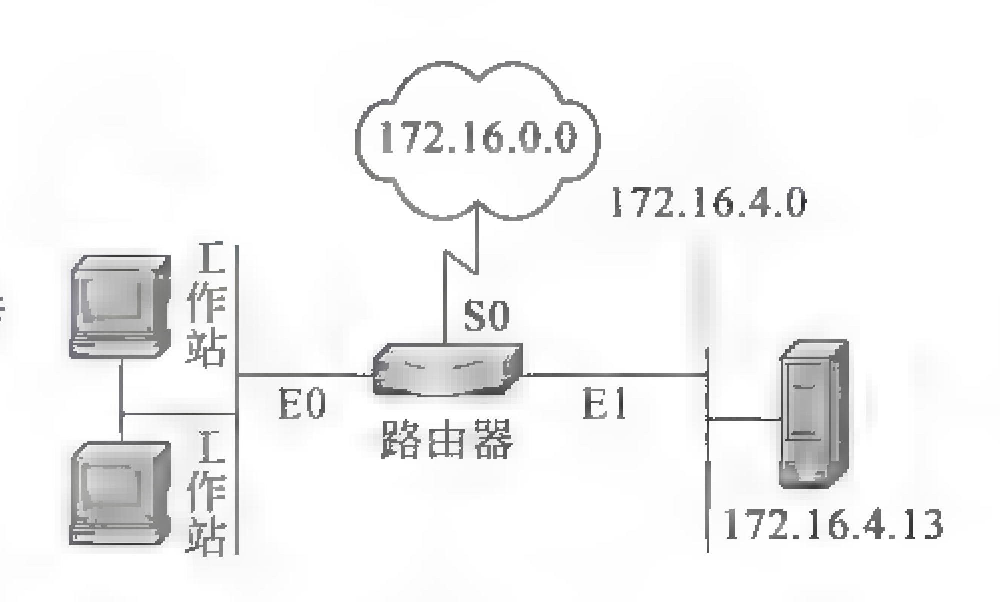


图 4-6　例 4-1 的图

(2) 将 ACL 绑定到 E0 和 E1 的出口上,命令如下:

```
Router(config)#interface E0
Router(config-if)#  ip access-group 1 out
Router(config)#interface E1
Router(config-if)#ip access-group 1 out
```

例 4-2 阻止特定地址。

阻止来自于特定地址 171.16.4.13 的数据流,其他数据流被转发到以太网口 E0。

(1) 创建标准 ACL,命令如下:

```
Router(config)#access-list 1 deny 171.16.4.13 0.0.0.0
Router(config)#access-list 1 permit any
```

(2) 绑定,命令如下:

```
Router(config)#interface E0
Router(config-if)#ip access- group1 out
```

第一条 access-list 命令用 deny 参数来禁止来自于这个指定主机的数据流,地址掩码 0.0.0.0 表明要检查匹配地址中的所有位。

在第二条 access-list 命令中,0.0.0.0 255.255.255.255 地址和通配符掩码组合,表示允许来自于任何源地址的数据流。这个组合也可以用关键字 any 替代。在地址中,全 0 表示占位符,通配符掩码中的全 1 表示地址中的 32 位都不会被检查。任何一个不匹配第一条指令的数据包将匹配第二条指令。

例 4-3 阻止特定的子网。

阻止来自于特定子网 171.16.4.0 的数据通过 E0 端口,而转发其他数据。

(1) 创建 ACL,命令如下:

```
Router(config)#access-list 1 deny 171.16.4.0 0.0.0.255
Router(config)#access-list 1 permit any
```

(2) 绑定,命令如下:

```
Router(config)#interface E0
Router(config-if)#ip access-group1 out
```

4.2.7 扩展 ACL 的配置

扩展 ACL 提供了比标准 ACL 更大范围的控制,因而运用更广。例如,可以使用扩展 ACL 来实现允许 Web 数据流而禁止 FTP 或 Telent。扩展 ACL 可以检查源地址和目标地址、特定协议、端口号以及其他参数,更加灵活地描述 ACL 的任务,一个数据包可以根据它的源或者目的地址而被允许或者禁止。例如,扩展 ACL 可以允许来自 E0 要送到 S0 的 E-mail 数据,而禁止远程登录或者文件传输。

假设端口 E0 与一个扩展 ACL 相关联,可以使用精确的逻辑指令来创建 ACL。在数

据包进入这个端口之前，相应的 ACL 将对其进行检查。

基于扩展 ACL 检查，数据包将被允许或禁止。对于进入端口的数据，允许的数据包将被继续处理；对于发出端口的数据，允许的数据包将被转发到 E0 端口，拒绝的数据包将被丢弃，某些协议还会向发送方传送数据包，说明目标不可到达。

一个 ACL 中可以包含任意多条指令，每一条指令应该具有相同的标识名或者数字。ACL 中的指令越多，就越难理解和管理。所以，为 ACL 做好文档可以防止混淆。

标准 ACL（数字 1～99）可以提供数据流过滤控制，这是基于源地址和掩码实现的。标准 ACL 可以允许或禁止整套 IP 协议。

为了进行更加精确的数据流过滤，需要扩展 ACL。扩展 ACL 检查源地址和目标地址，以及 TCP 或 UDP 端口号，还可以指定扩展 ACL 针对特定的协议进行操作。扩展 ACL 使用的数字范围是 100～199。

扩展 ACL 的配置步骤为：创建扩展 ACL，然后绑定到某个端口。

如表 4-5 所示，这里给出的创建 ACL 的命令并没有包含全部参数和选项。表 4-6 列出了常用的端口号。

表 4-5　扩展 ACL 的配置

命　　令	说　　明
Router(config)# access-list access-list-number [permit | deny] protocol source source-mask [operator port] destination destination-mask[operator port]	创建一个扩展 ACL，参数说明如下： access-list-number：100～199 的数字用于标志 ACL protocol 可以是 IP、TCP、UDP、ICMP、GRE 或 IGRP source 和 source-mask：源地址和源掩码 operator port：TCP 的操作端口号，可以是 lt(小于)、gt(大于)、eq(等于)、neq(不等于)某个端口号 destination 和 destination-mask：目的地址和目的掩码
Router(config-if)# ip access-group access-list-number[in|out]	绑定 ACL 到某个接口上
Router# show access-list access-list-number	显示 ACL 包含的命令语句
Router# show ip interface 接口标识	查看是否为某个接口绑定了 ACL

表 4-6　常用的端口号

常见的端口号	IP 协议	常见的端口号	IP 协议
20	FTP	25	SMTP
21	FTP	53	DNS
23	Telnet	69	TFTP

例 4-4　使用扩展 ACL。

要求只有主机 172.16.1.1 能够通过 FTP 访问网络 192.168.1.0，如图 4-7 所示。

(1) 创建扩展 ACL,命令如下:

```
Router(config)#access-list 100 permit TCP 172.16.1.1 0.0.0.0 192.168.1.0 0.0.0.255 eq 20
```

(2) 将 ACL 绑定到 E2 的出口命令如下:

```
Router(config)#interface E2
Router(config-if)#ip access-group 100 out
```

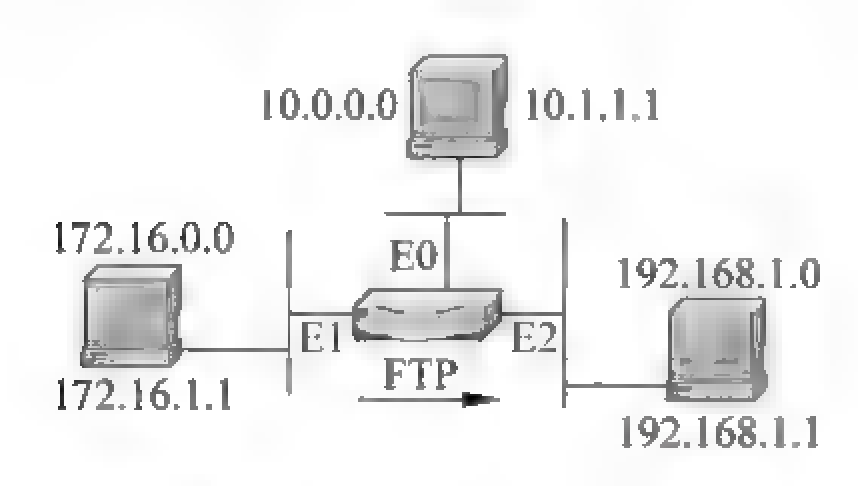


图 4-7 例 4-4 的图

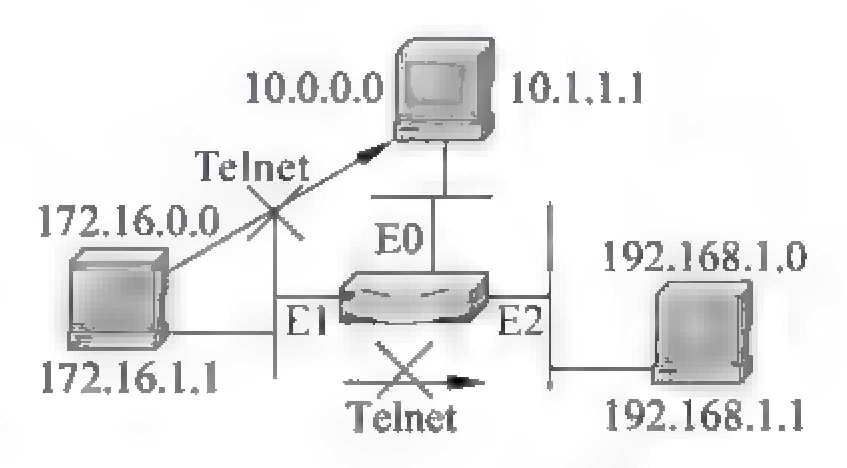


图 4-8 例 4-5 的图

例 4-5 使用扩展 ACL。

拒绝网络 172.16.0.0 通过 Telent 访问任何网段,允许其他所有 IP 数据流,如图 4-8 所示。

(1) 创建扩展 ACL,命令如下:

```
Router(config)#access-list 101 deny tcp 172.16.0.0 0.0.255.255 any eq 23
Router(config)#access-list 101 permit ip any any
```

命令行中的第一个 any 为源地址,第二个 any 为目的地址,两个 any 表示源和目的都为任意。

(2) 绑定 ACL 到 E1 的出口,命令如下:

```
Router(config)#interface E1
Router(config-if)#ip access-group 101 in
```

例 4-6 使用扩展 ACL。

禁止网络 192.168.1.0 使用 ping 命令访问网络 172.16.0.0,允许其他 IP 数据流,如图 4-9 所示。

(1) 创建扩展 ACL,命令如下:

```
Router(config)#access-list 199 deny icmp 192.168.
1.0 0.0.0.0 172.16.0.0 0.0.255.255
Router(config)#access-list 199 permit ip any any
```

(2) 绑定 ACL,命令如下:

```
Router(config)#interface E1
Router(config-if)#ip access-group 199 out
```

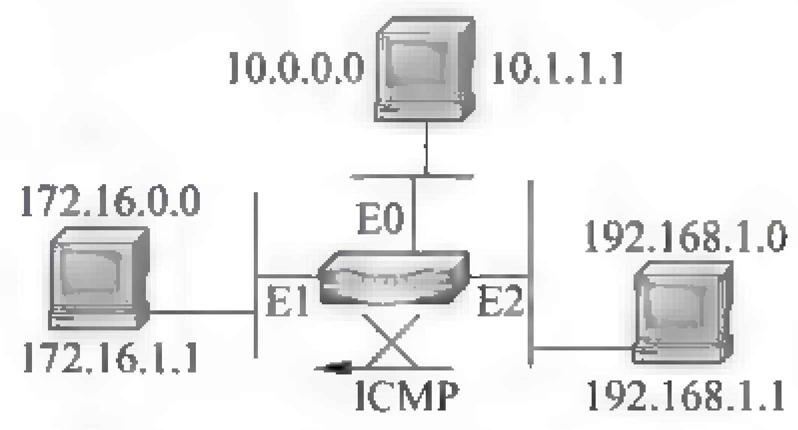


图 4-9 例 4 6 的图

4.2.8　命名 ACL 的配置

可以使用字符串代替数字来标识 ACL，称为命名(Named)ACL。命名 ACL 作为一种特殊的 ACL，具有很多优点：

① 可以用有含义的字符串直观地标识一个 ACL。

② 在路由器上，对于给定的协议，当需要的配置超出了 99 个标准 ACL 或者 100 个扩展 ACL 时，可以采用命名 ACL。

③ 可以在不删除整个 ACL 的情况下修改 ACL 中的某一条语句。

在使用命名 ACL 的时候，需要考虑到以下因素：

① 命名 ACL 与 Cisco IOS 11.2 之前的版本不兼容。

② 命名 ACL 也包含标准和扩展 ACL。

③ 不能为多个 ACL 使用相同的名字。不同类型的 ACL 不能使用相同的名字。

为了给一个 ACL 命名，可以使用表 4-7 所示的命令。

表 4-7　命名 ACL 配置

命　令	说　明
Router(config) # ip access-list[standard | extended]name	创建一个命名 ACL，参数 standard 和 extended 指明了是标准还是扩展 ACL，参数 name 是标识 ACL 的名称的字符串(命令执行后，进入如下模式：Router(config[std-|ext-nacl] #))
Router(config[std-|ext-nacl]) # [permit | deny]测试条件	向命名 ACL 写入命令语句
Router(config[std-|ext-nacl]) # no [permit | deny]测试条件	删除命令 ACL 中的某一条语句。注意，该 ACL 仍然存在，这与用数字标识的 ACL 不同
Router(config-if) # ip access-group name[in | out]	绑定命名 ACL

例 4-7　使用标准命名 ACL。

如例 4-1 所示，现在改为使用命名 ACL 完成任务。

(1) 创建命名 ACL，命令如下：

```
Router(config)#access-list standard ex19
Router(config std-nscl)#permit 171.16.0.0 0.0.255.255
```

(2) 将 ACL 绑定到 E0 和 E1 的出口，命令如下：

```
Router(config)#interface E0
Router(config-if)#ip access-group ex19 out
Router(config )#interface E1
Router(config-if)#ip access group ex19 out
```

例 4-8 使用扩展命名 ACL。

如例 4 5 所示，现在改为使用命令 ACL 完成任务。

(1) 创建命名 ACL，命令如下：

```
Router(config)#access-list standard ex17
Router(config std-nacl)#deny tcp 172.16.0.0 0.0.255.255 any eq 23
Router(config std-nacl)#permit any any
```

(2) 绑定 ACL，命令如下：

```
Router(config)#interface e1
Router(config-if)#ip access-group ex17 in
```

任务 4.3 设置防火墙

任务回顾：用户希望在机房对防火墙进行初始配置后，通过 Web 方式对防火墙进行远程配置和管理。对于硬件防火墙，以锐捷的产品来介绍。

所需设备为 RG-WALL 150 防火墙(1 台)、主机(1 台)、直连线(1 条)，组网方式如图 4-10 所示。

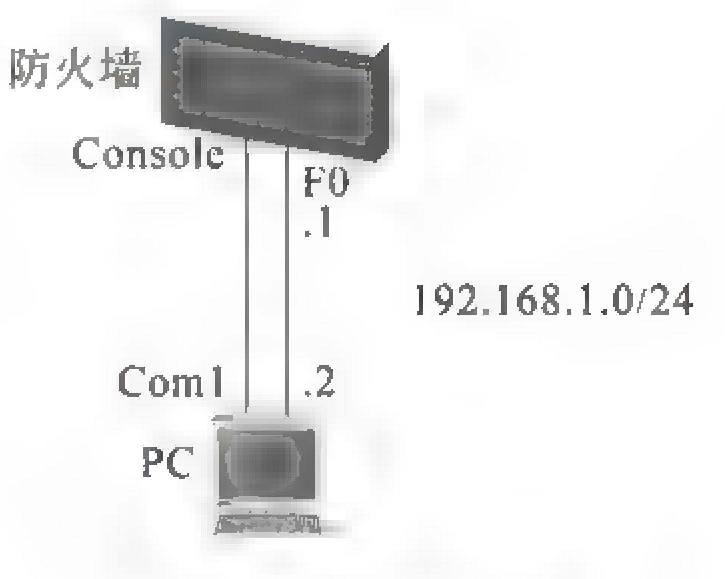


图 4-10 防火墙拓扑图

1. 登录防火墙

```
***********************************************
** RG-OS V1.0 http://www.red-giant.com.cn **
***********************************************
RG-Wall-150 login: root
Password: rg-wall123
/>si                              !进入系统初始化设置
```

RG-WALL 默认登入的提示，或者重新设置时提示的内容如图 4-11 所示。

按任意键进入默认设置阶段。第 -步，系统将提示输入序列号、feature code 以及授权号。

① 输入序列号 SW xx xxxxx。请按照"产品使用授权书"上提供的信息输入序列号，区分大小写；序列号以 SW-xx-xxxxx 和 SK-xx-xxxxx 的格式输入。如图 4-12 所示。

② 输入 feature code。feature code 是设置 RG WALL 可使用功能的编码，是根据与锐捷公司签订合同提供的 16 位编码而定的。输入 feature code 后，出现如图 4 13 所示授权号输入提示。

③ 输入授权号，如图 4 13 所示。授权号与序列号和 feature code 相同，是锐捷公司赋予的编号。授权号输入错误，将不能继续安装。

④ 产品授权号输入正确后，将出现如图 4 14 所示的画面，进入下 -步设置阶段，请按任意键继续。



图 4-11　超级终端设置

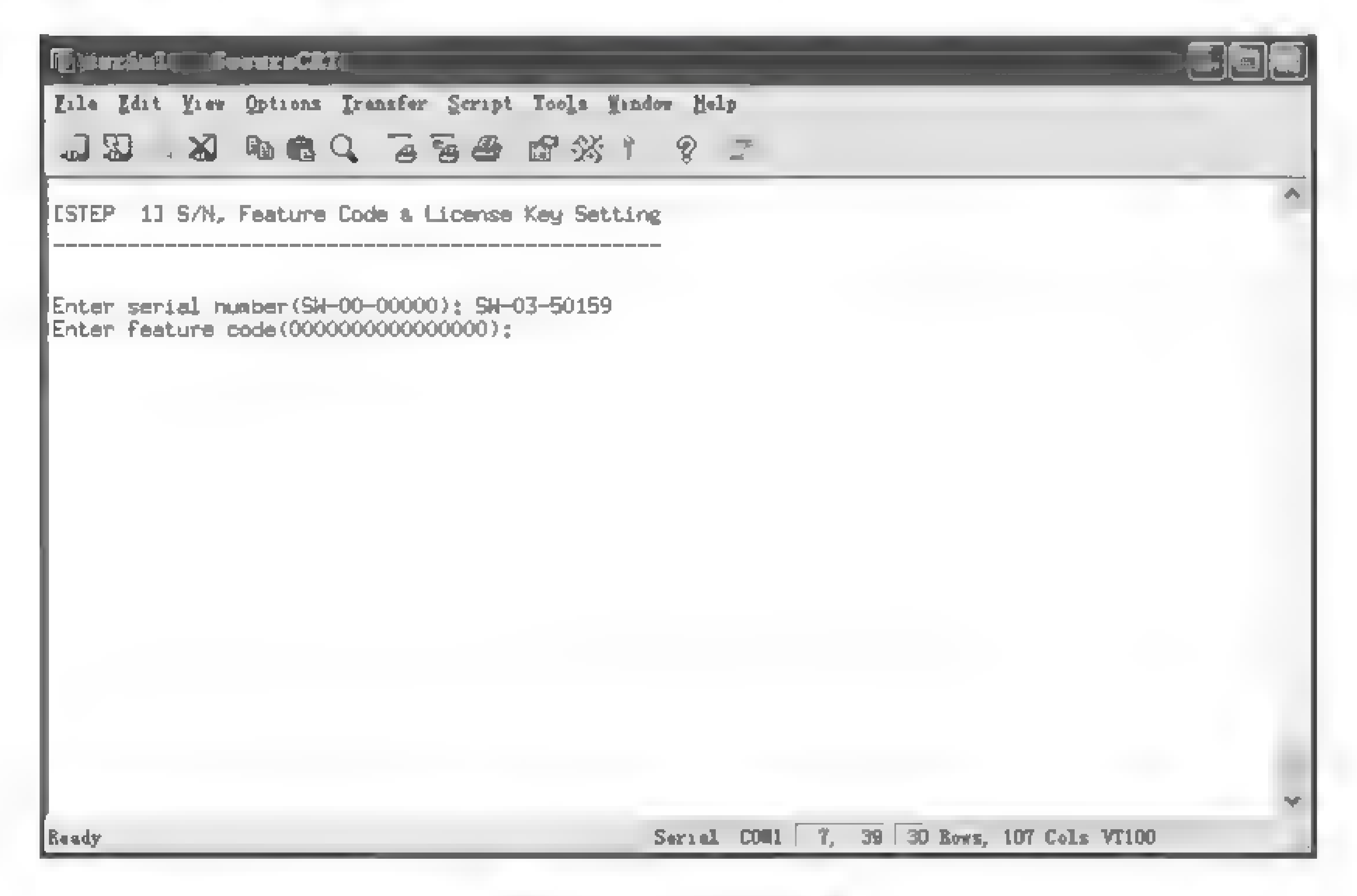


图 4-12　序列号设置

2. 选定防火墙的工作模式

防火墙的工作模式有路由模式(Router mode)和网桥模式(Bridge mode)两种,如图 4-15 所示。按 Enter 键将选择默认的路由模式。

注意: 这一阶段的选择决定以后防火墙的工作模式,决定 RG WALL 在安装网络中要起的作用。本节将说明防火墙在路由模式下的设置方法。

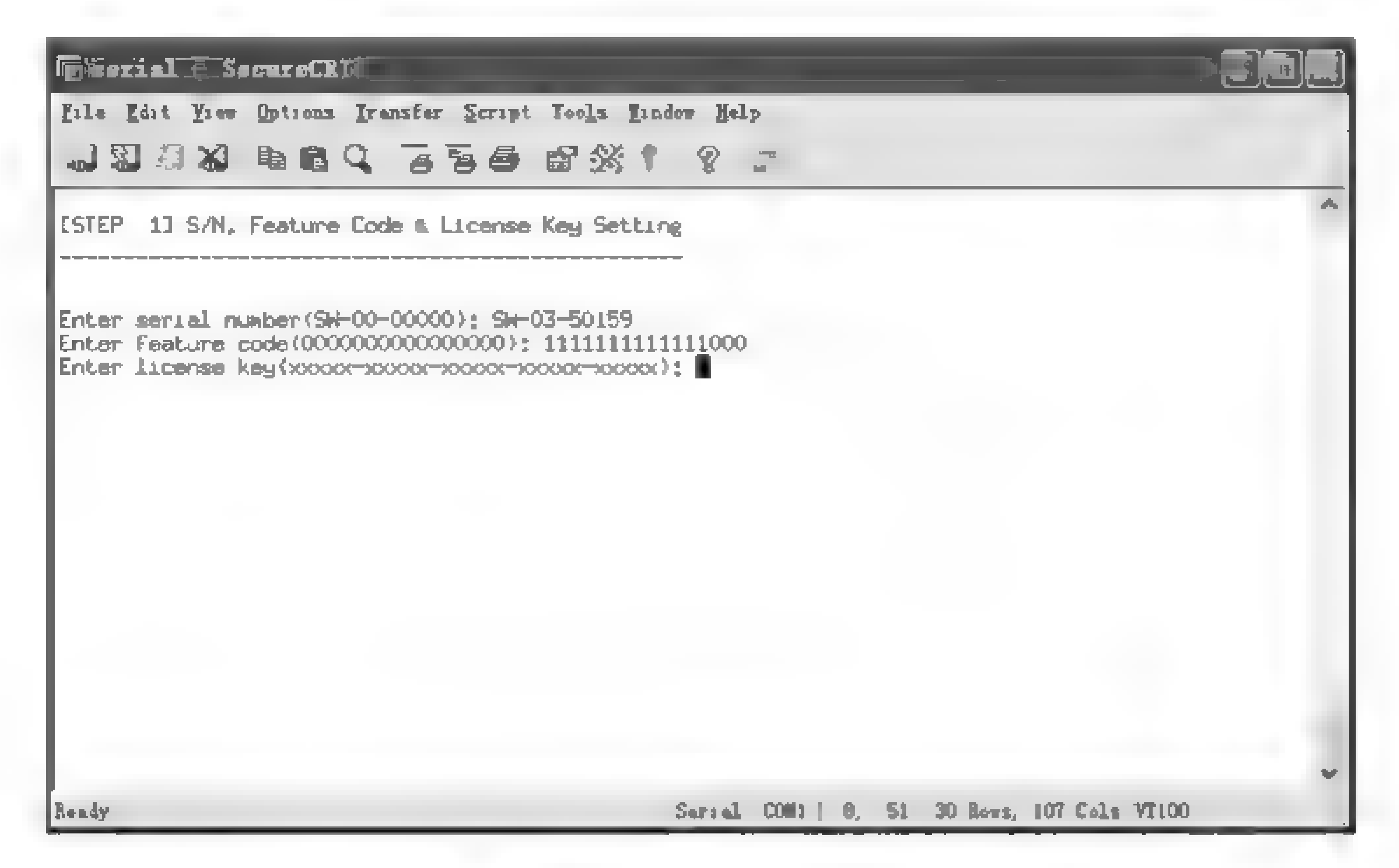


图 4-13　输入授权号

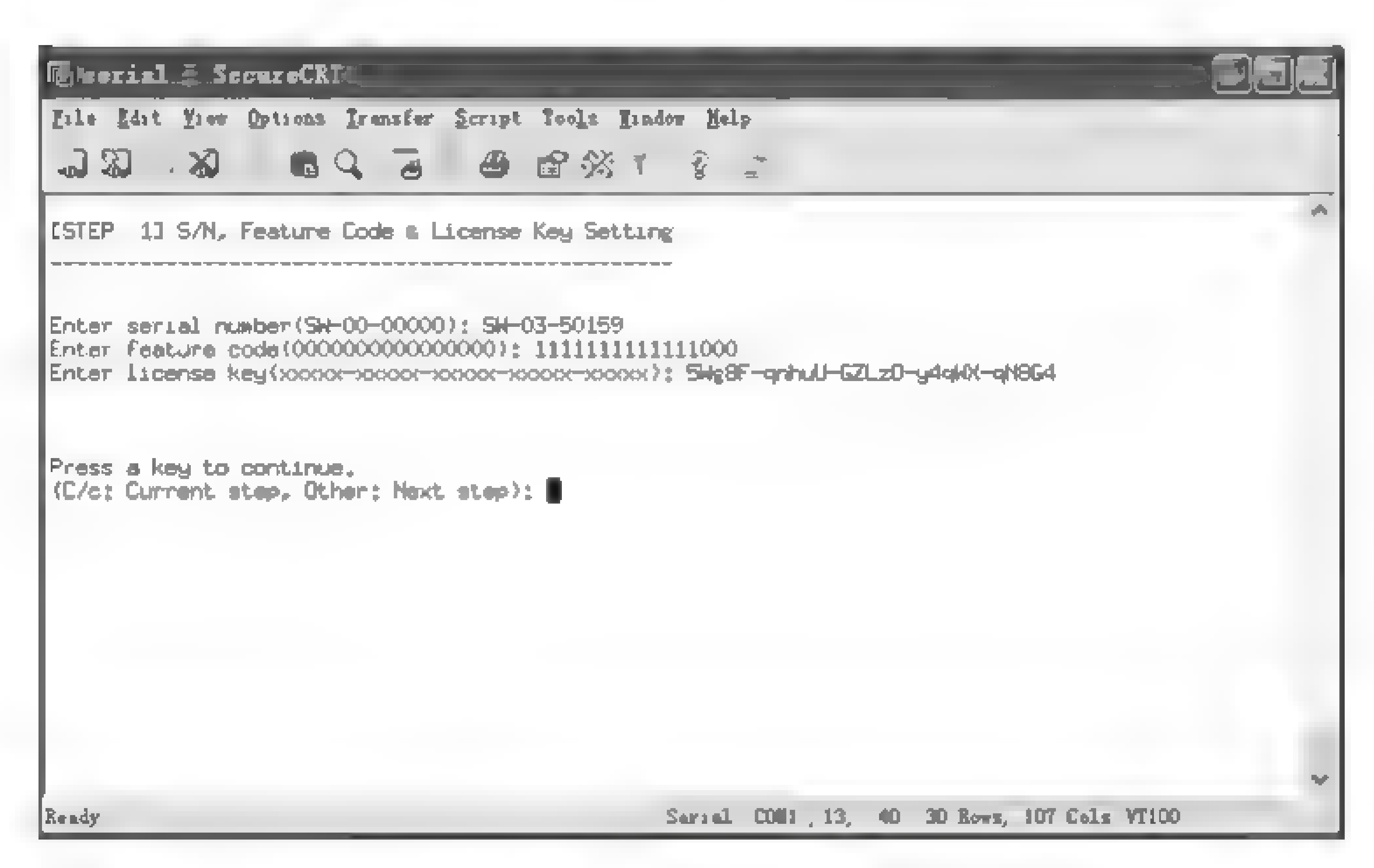


图 4-14　初始界面

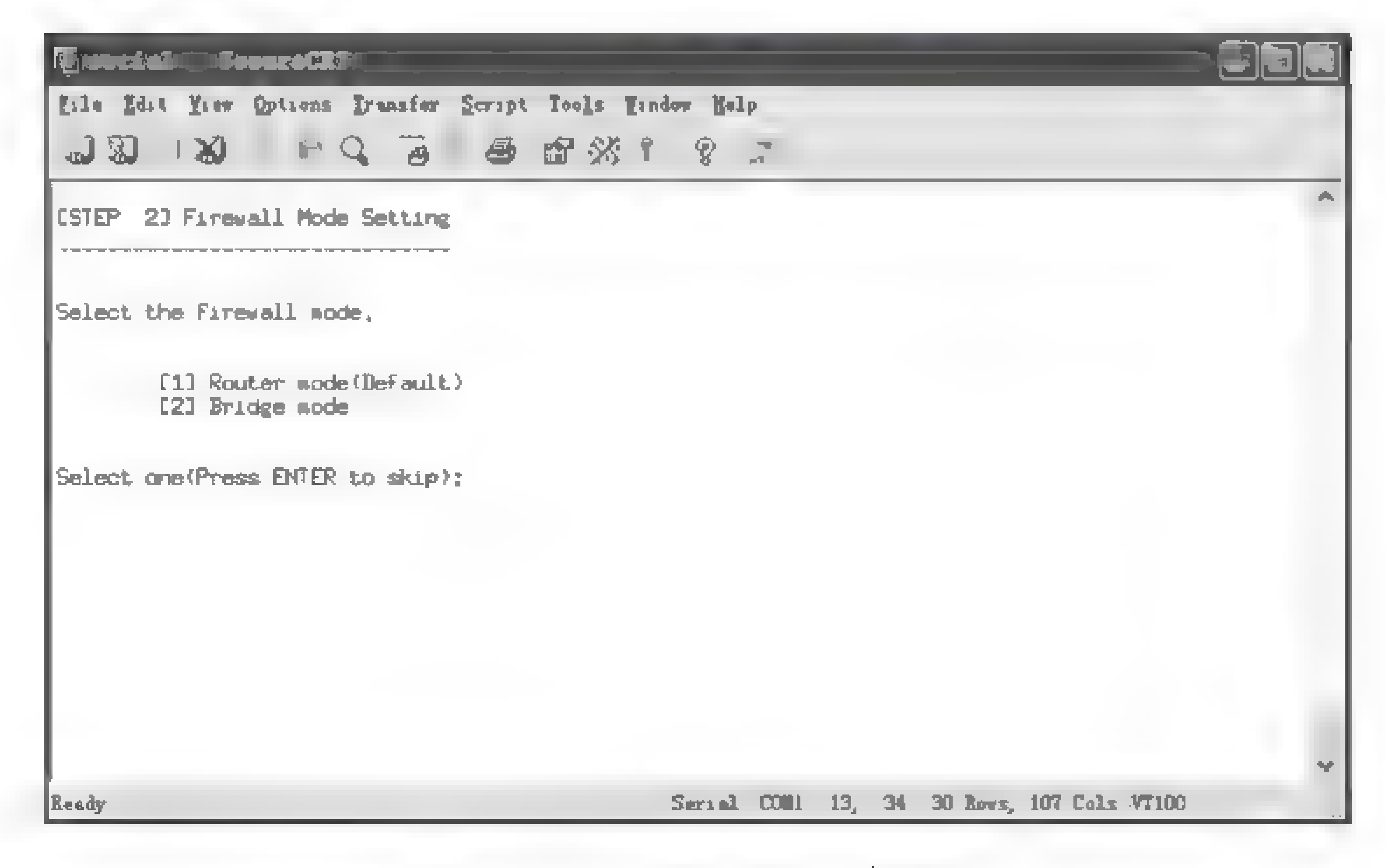


图 4-15　选定防火墙工作模式

图 4 16 所示是选择路由模式以后出现的画面。在选择路由模式后，进入下一个安装阶段。

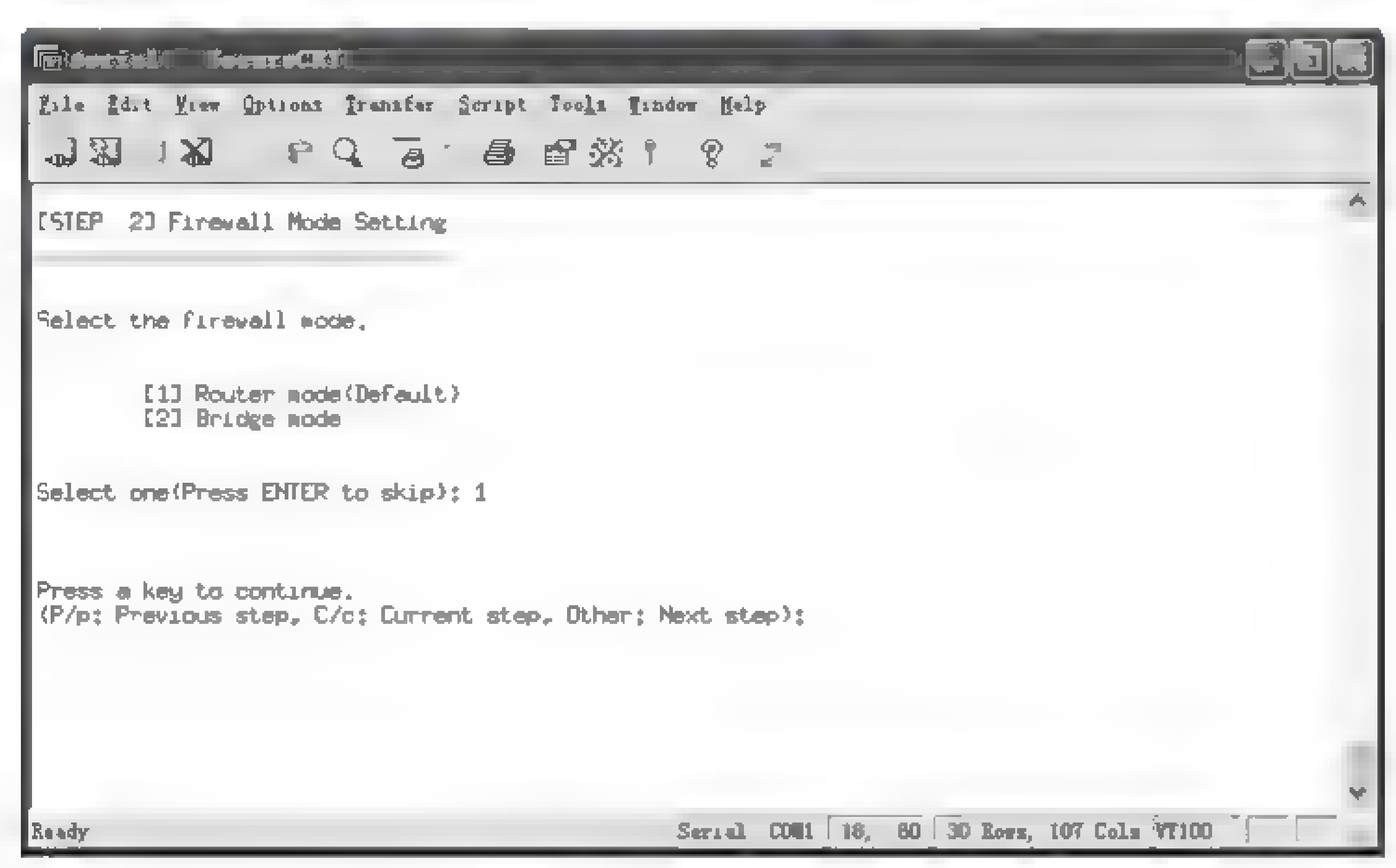


图 4-16　选择路由模式

在图 4-16 画面中出现以下输入提示：

① 输入 P 或 p 时，将取消当前设置和之前的设置，返回前一个设置阶段。

② 输入 C 或 c 时，将取消当前设置的内容，重新开始当前设置作业。即在现阶段，如果想重新选择系统模式，输入 C 或 c。

命令键不区分大小写，通常输入小写字母即可。

③ 输入任意键时，将应用当前设置内容，并进入下一个设置阶段。

本阶段的"取消"以及"移动"方法，与其他安装步骤相同。在以后的安装过程中，我们将省略说明。

3. 输入管理员 ID 和密码

完成防火墙模式设置以后，出现管理员输入画面，如图 4-17 所示。

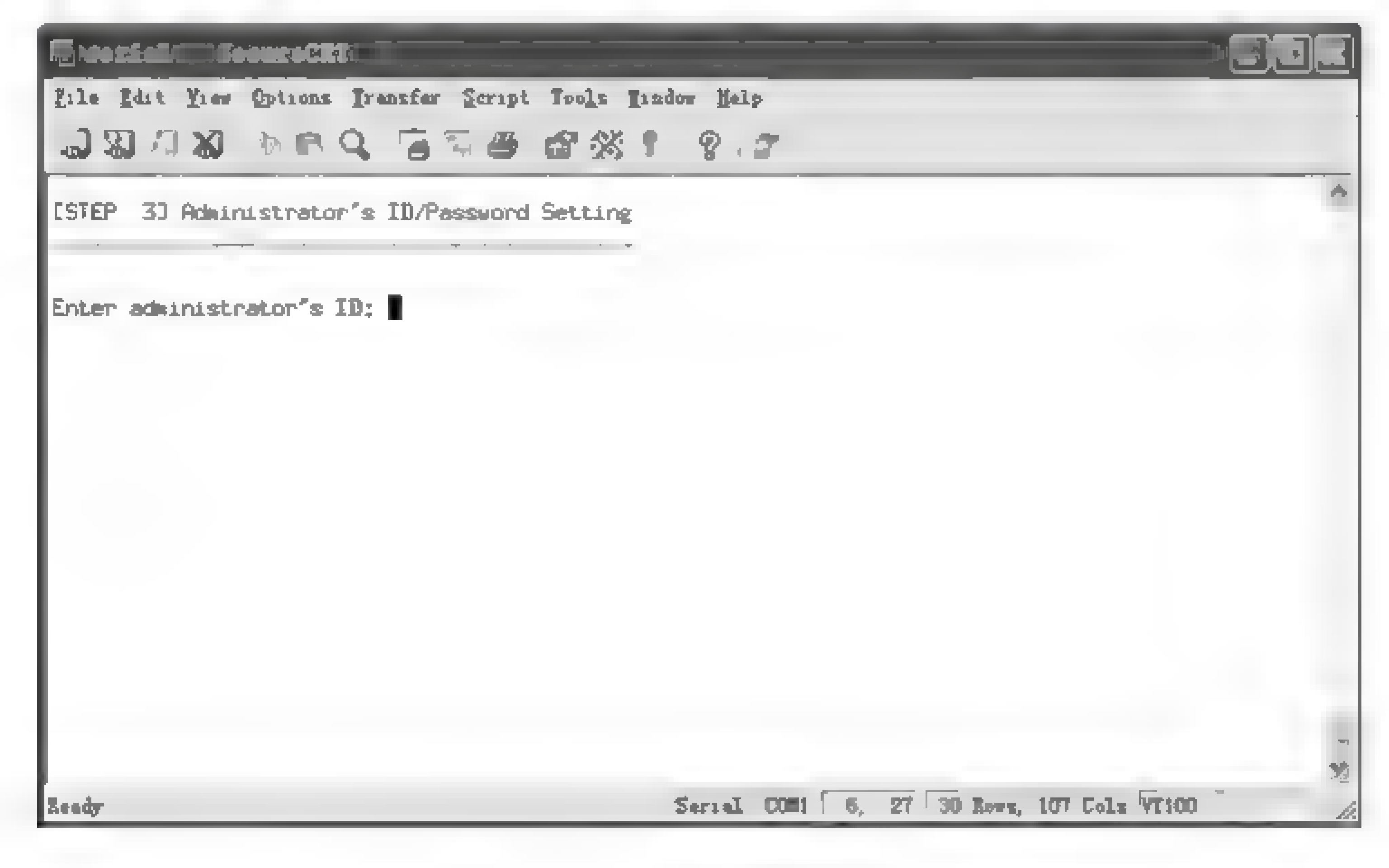


图 4-17　防火墙设置(1)

① 输入要启用的管理员 ID 号：admin。这里的管理员表示带有停止/启动系统、授权其他管理员权限的主要系统负责人员账号，admin 一般作为管理员的账号。

② 输入管理员账号所配套的密码：admin123，如图 4-18 所示。管理员密码必须是英文和数字的混合格式，而且必须多于 6 个字。通过管理员 GUI 输入同样的密码登录超过 20 次以上时，系统会要求修改密码。

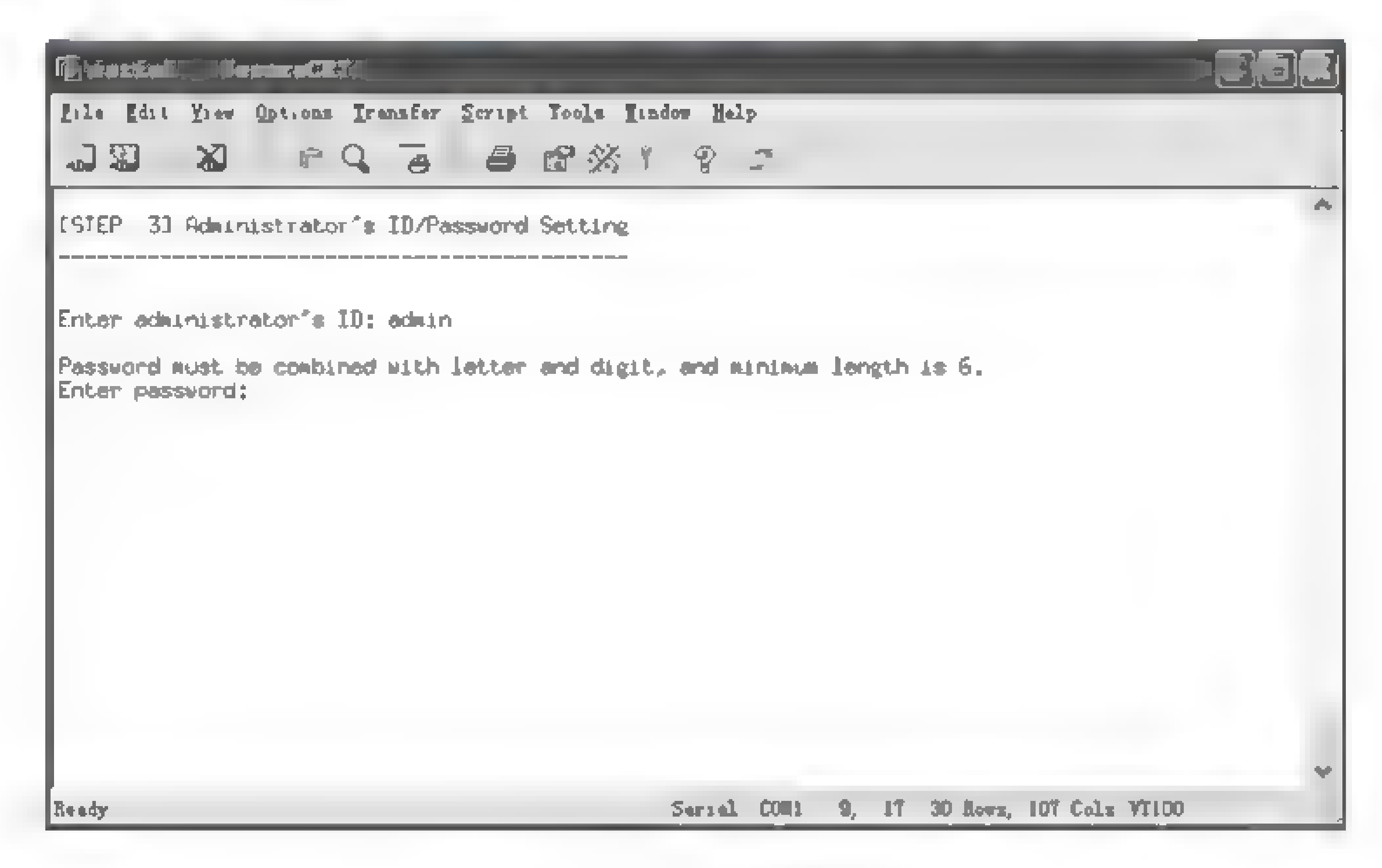


图 4-18　防火墙设置(2)

③ 确认密码：admin123，如图 4-19 所示。输入密码以后，为了确认密码是否匹配，出现重复输入密码的提示。两次密码输入完全匹配时，才可以进行下一步操作。

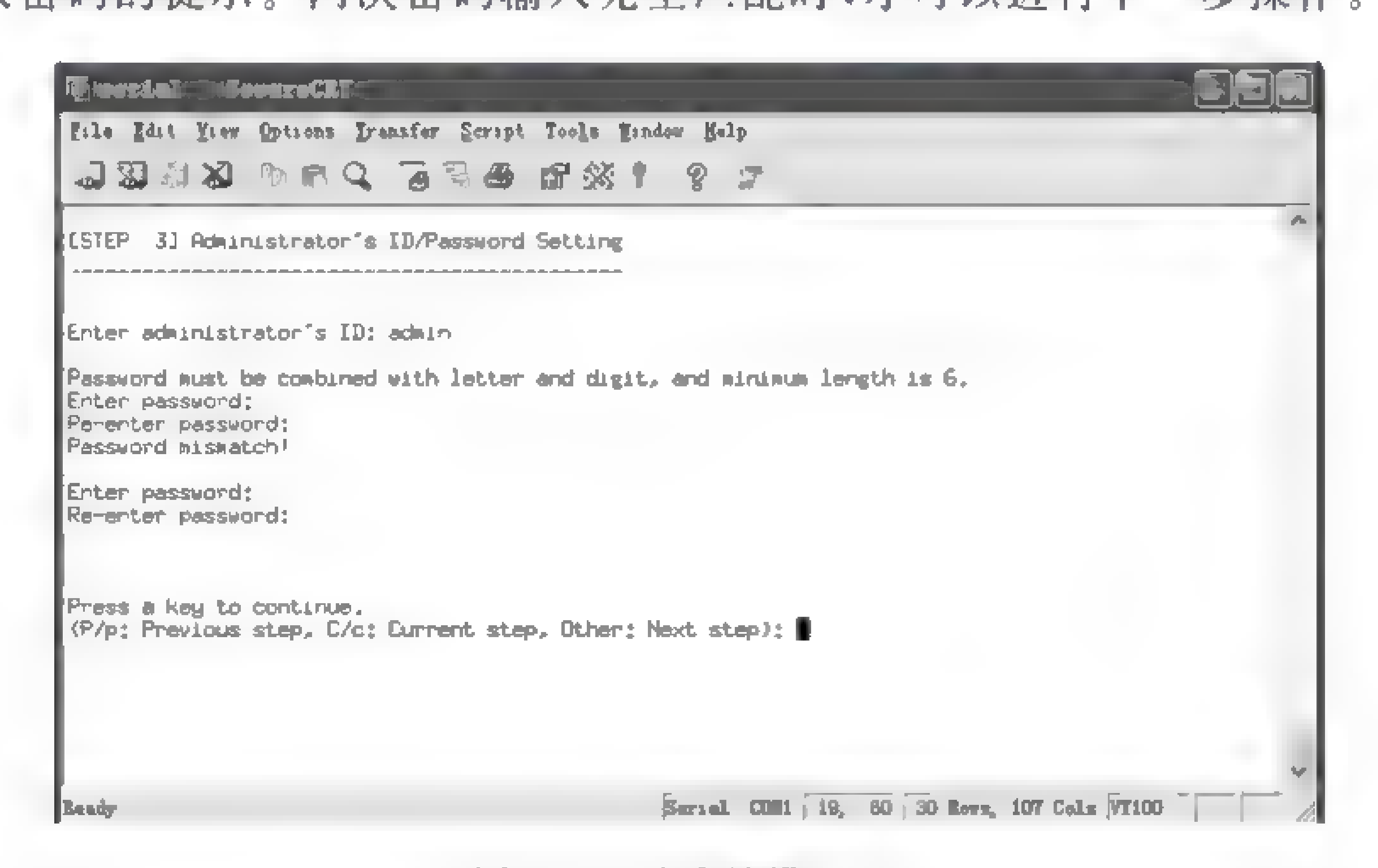


图 4-19　防火墙设置(3)

4. 设置系统名称以及语言

① 输入系统名称：Host. firewall. com，如图 4-20 所示。

② 选择 CLI Terminal 识别的语言，默认值是中文，如图 4-21 所示。输入“1”并按 Enter 键，进入下一个阶段。

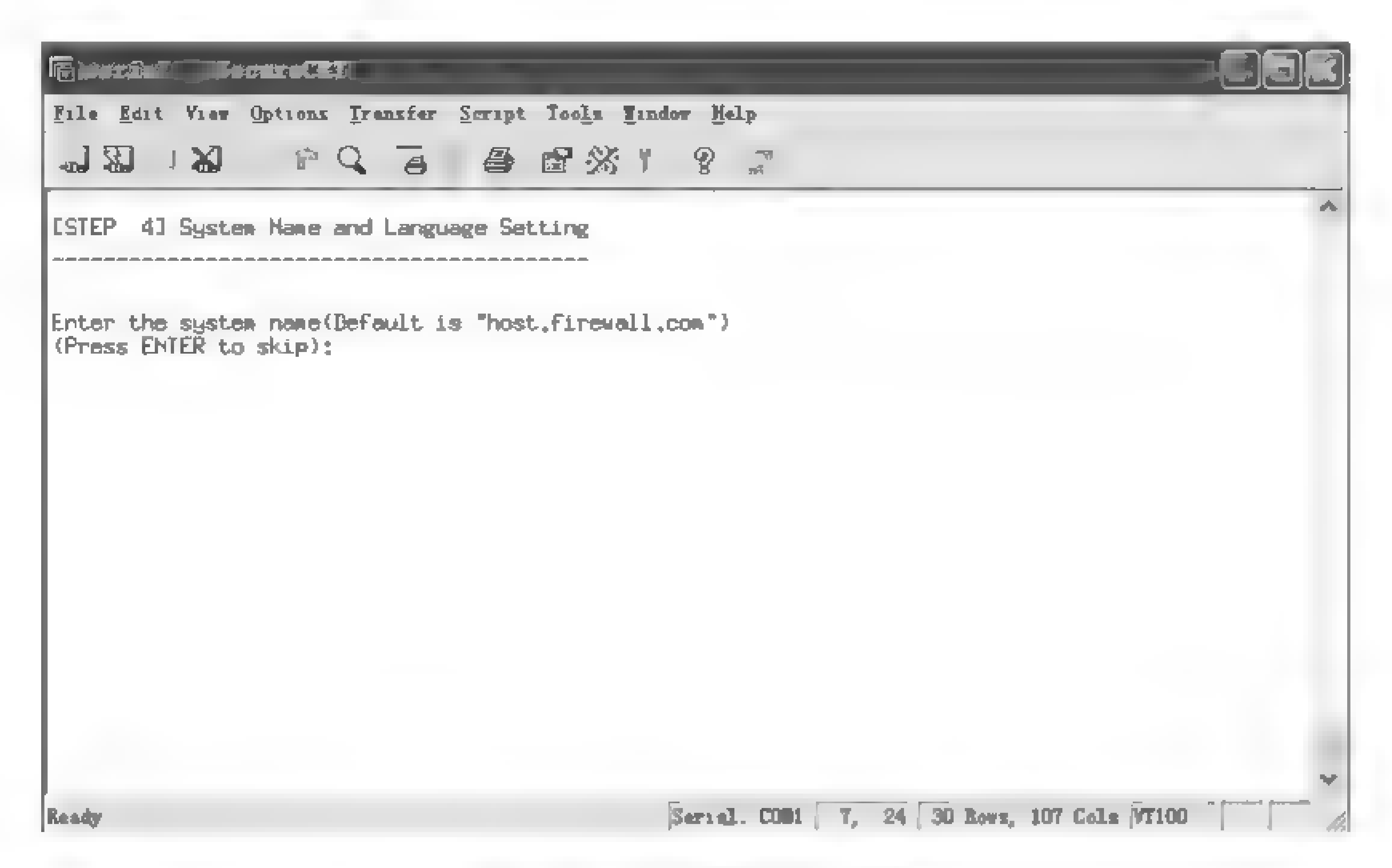


图 4-20　防火墙系统设置

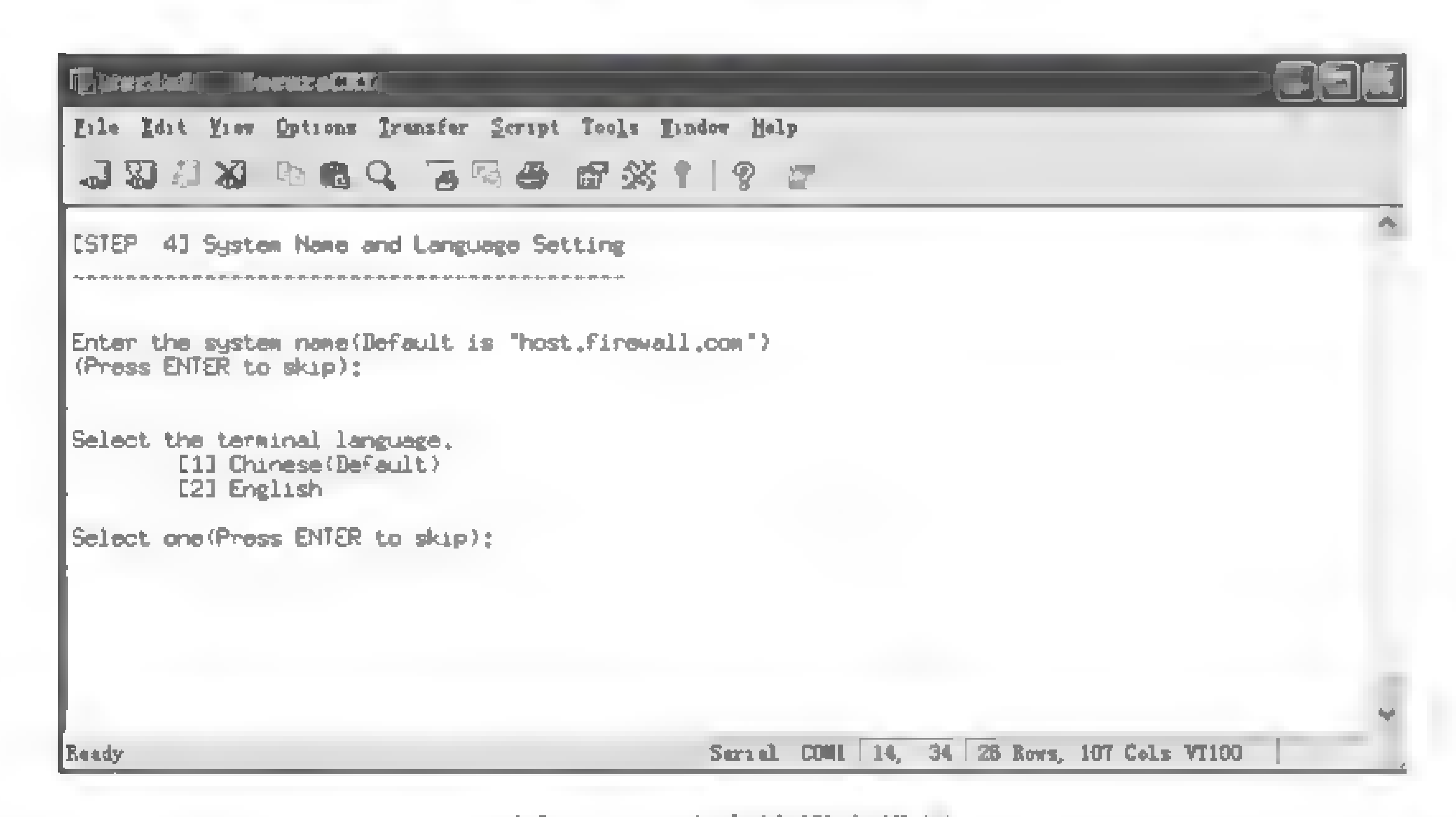


图 4-21　防火墙语言设置

5. 设置时间

所有的日志和报表以及计划任务的作业都会根据设置的时间来形成，因此必须正确输入当前时间。选择默认[0]，如图 4-22 所示，确认后进入下一个阶段。

6. 指定管理员 PC 的 IP 地址

配置管理员 PC 的 IP 地址为 192.168.1.10，192.168.1.100。

RG WALL 提供的服务包括允许向特定管理员 IP 地址提供 SSHTTP，red giantguid 服务。想利用 RG-WALL 的 GUI 以及 CLI，必须注册管理员 PC 的 IP 地址。

管理员 PC 的 IP 地址可以最多输入 10 个，并且每个 IP 地址之间用逗号和空格隔开。输入管理员 IP 地址后进入下一阶段，如图 4-23 所示。

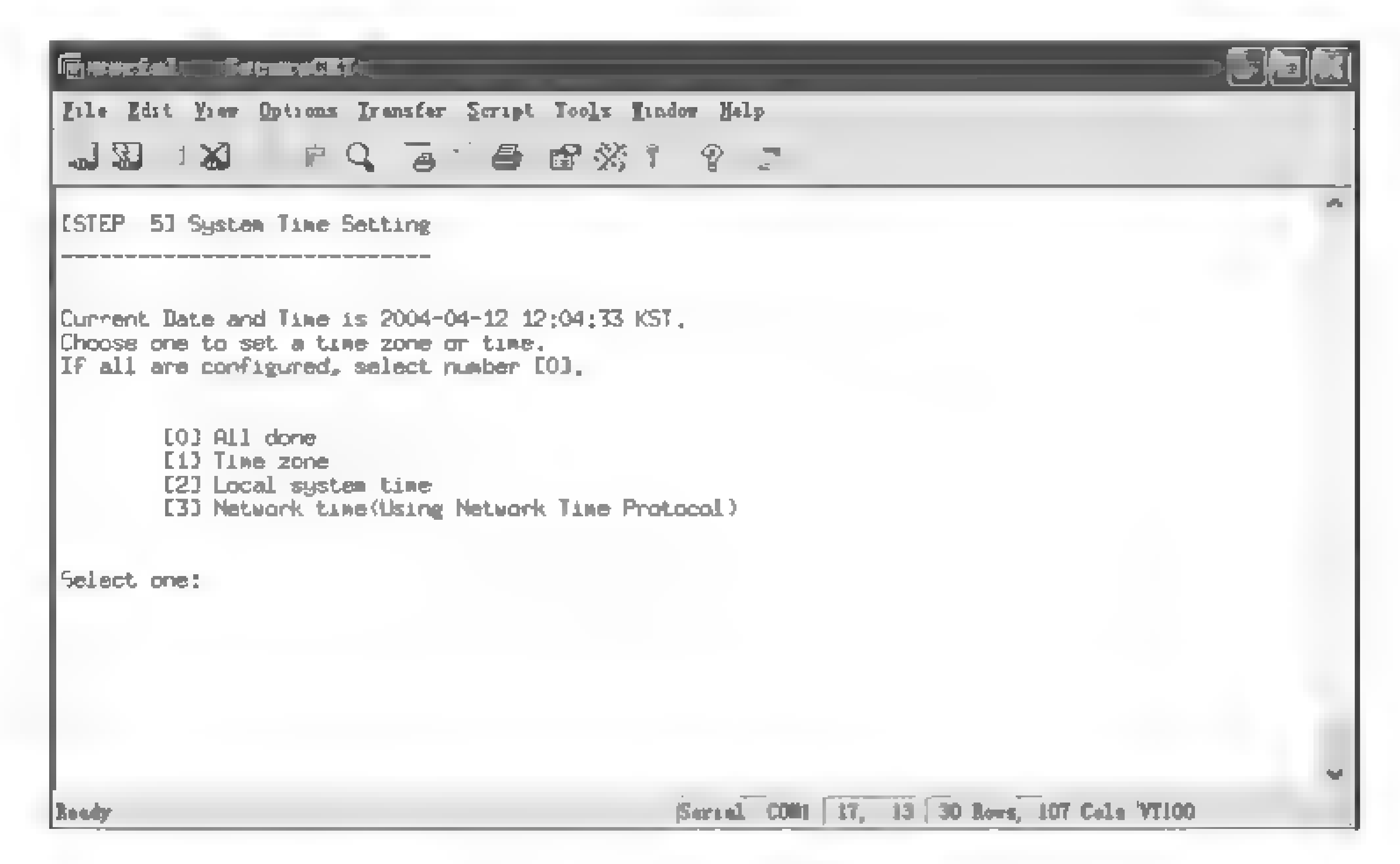


图 4-22 防火墙时间设置

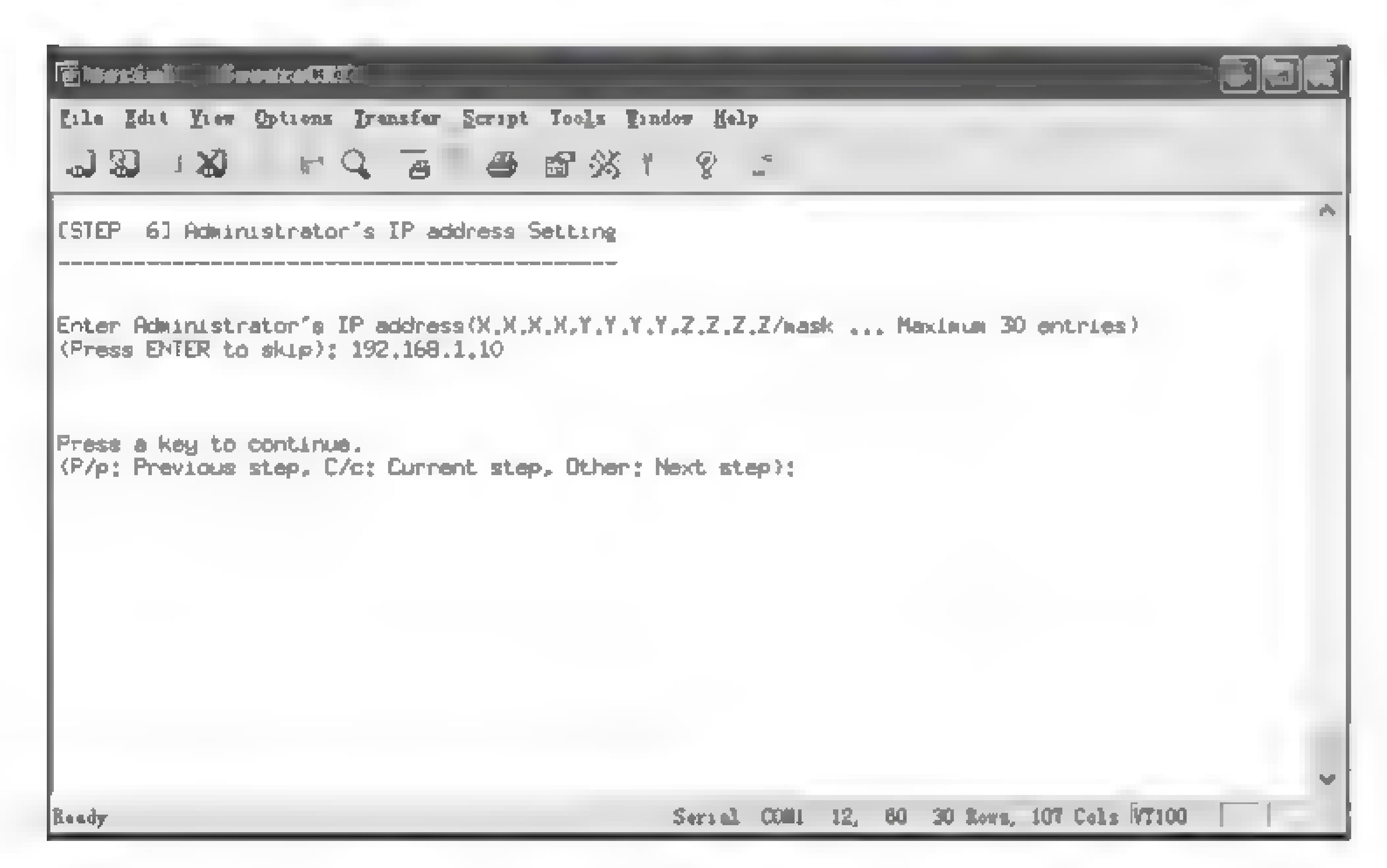


图 4-23 输入管理员 PC 的 IP 地址

7. 网络接口构成

为使 RG WALL 的网络连接正常，必须按照计划书的方案分配各接口地址。

显示当前接口设置以及选择接口的画面如图 4 24 所示。各接口的区域分配可以修改，但是必须设置 Internal 和 External，并且启用 HA 时必须设置 HA Link。

正确设置所有接口以后，选择[0]进入下一阶段。输入要修改的接口号，以修改设置。

选择需要修改的接口，出现如图 4 25 所示设置各接口内容的画面。选择其内容项后输入正确的值。

正确输入所有接口内容后选择[0]，继续设置其他接口。

8. 配置 VLAN

① 输入 VLAN 设置的接口号，开始设置 VLAN，如图 4 26 所示。

```
Serial - SecureCRT
File Edit View Options Transfer Script Tools Window Help

[STEP  7] Network Interface Setting
----------------------------------

Choose one to configure among these NICs.
If all are configured, select number [0].

        [0] All done
        [1] eth0    Zone: DMZ           MTU: 1500   Type: 100 Mbps
                    IP:                     Mask:
        [2] eth1    Zone: Internal      MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:
        [3] eth2    Zone: External      MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:
        [4] eth3    Zone: HA            MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:
        [5] eth4    Zone: Not Assigned  MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:
        [6] eth5    Zone: Not Assigned  MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:
        [7] eth6    Zone: Not Assigned  MTU: 1500   Type: 65535 Mbps
                    IP:                     Mask:

Select one:
Ready                              Serial  COM1  24,  13  30 Rows, 107 Cols  VT100
```

图 4-24　防火墙设置(1)——选择接口

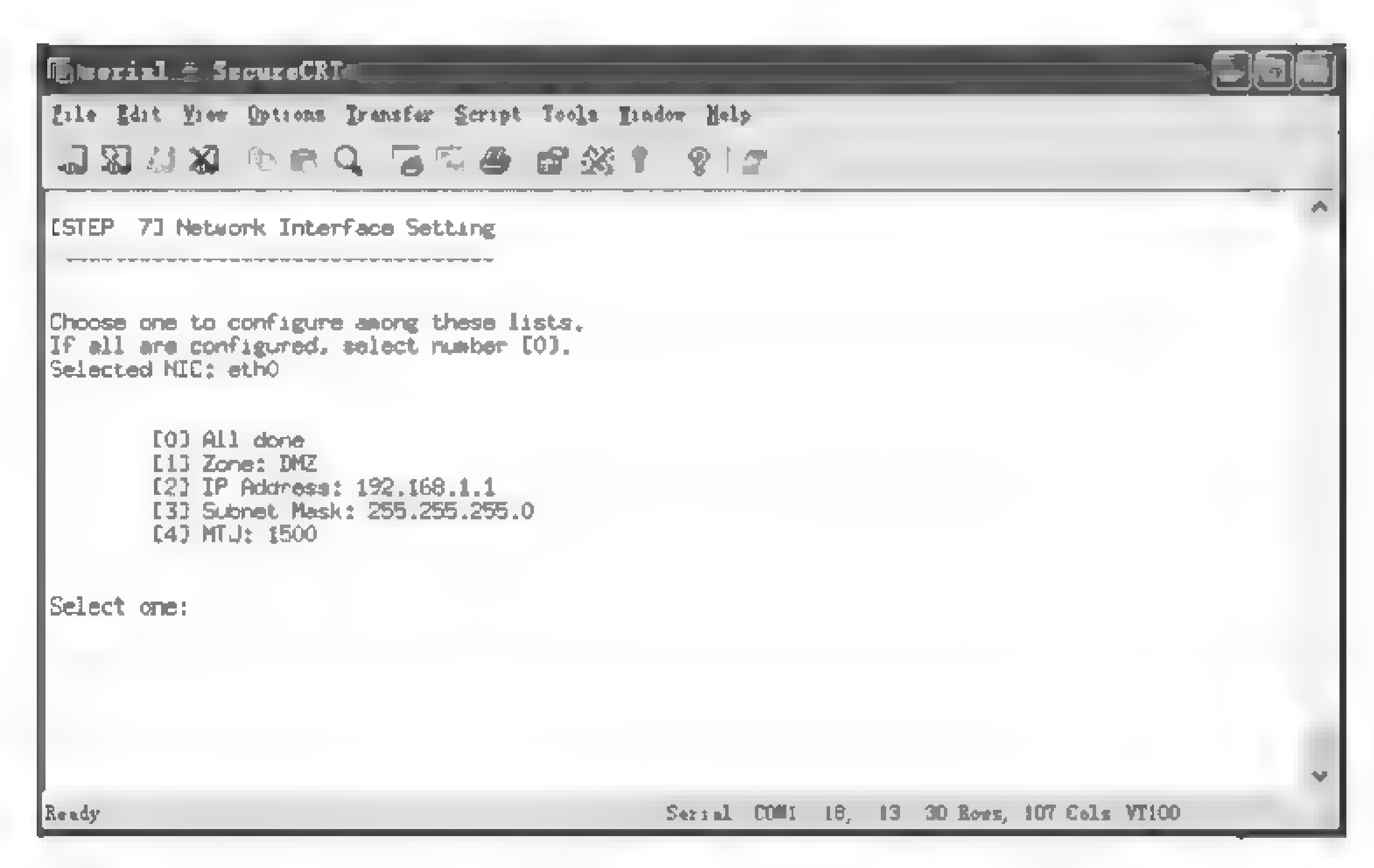


图 4-25　防火墙设置(2)——修改接口

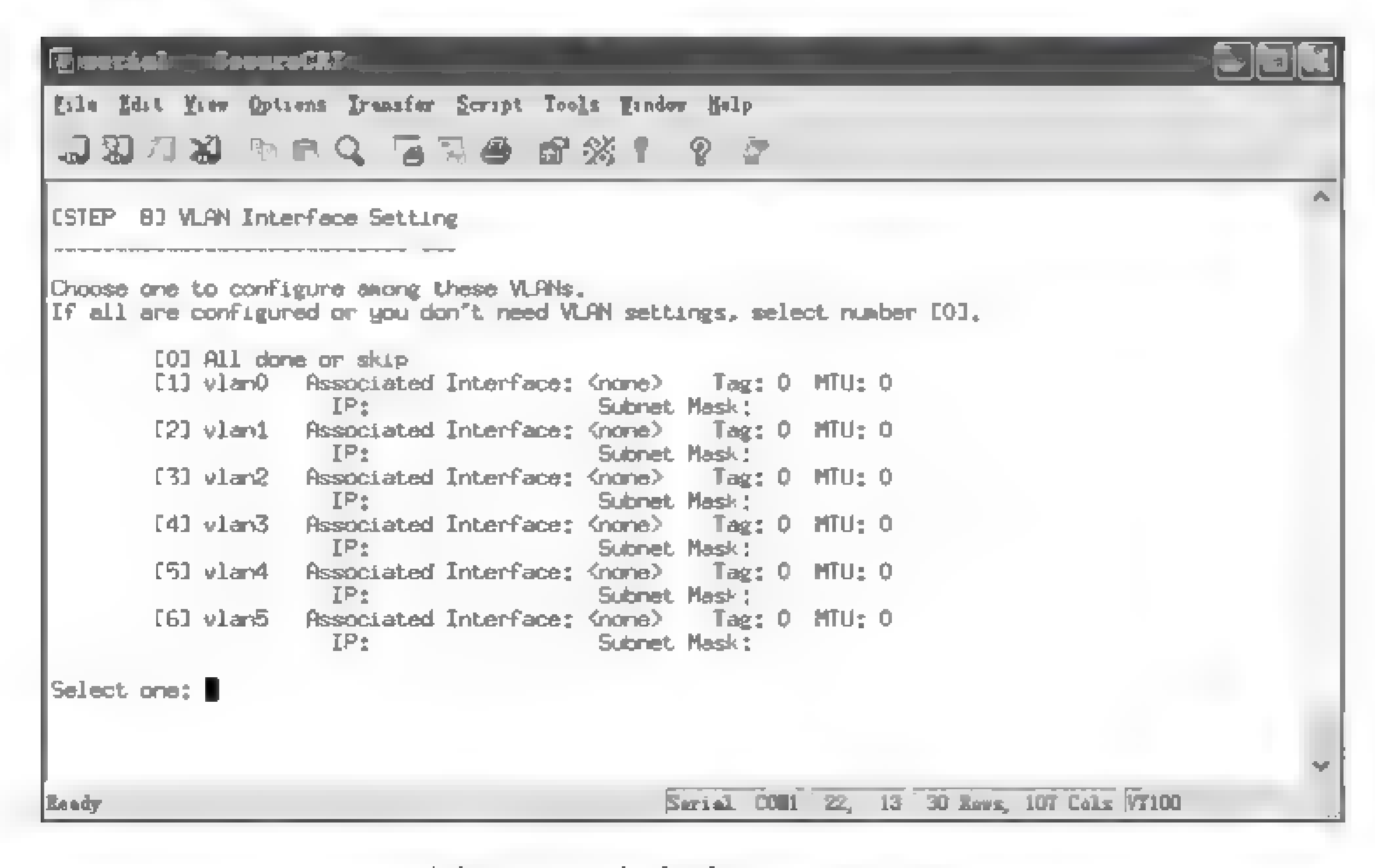


图 4 26　防火墙 VLAN 配置

② VLAN 设置完成后选择[0],进行下一个设置阶段。

如果要构成 VLAN 并通过 802.1q 方式访问,必须设置各 VLAN 的 IP 地址以及子网掩码和 MTU 信息。RG-WALL 共提供 6 个 VLAN 接口。图 4-26 所示画面只在路由模式下出现。

9. 设置静态路由

如果计划在路由模式下启用 OSPF,可以跳过这一阶段,进入 OSPF 设置阶段,或者以后通过 Web 方式设置。设置 RG-WALL 外部网的默认路径:Default Gateway,如图 4-27 所示。

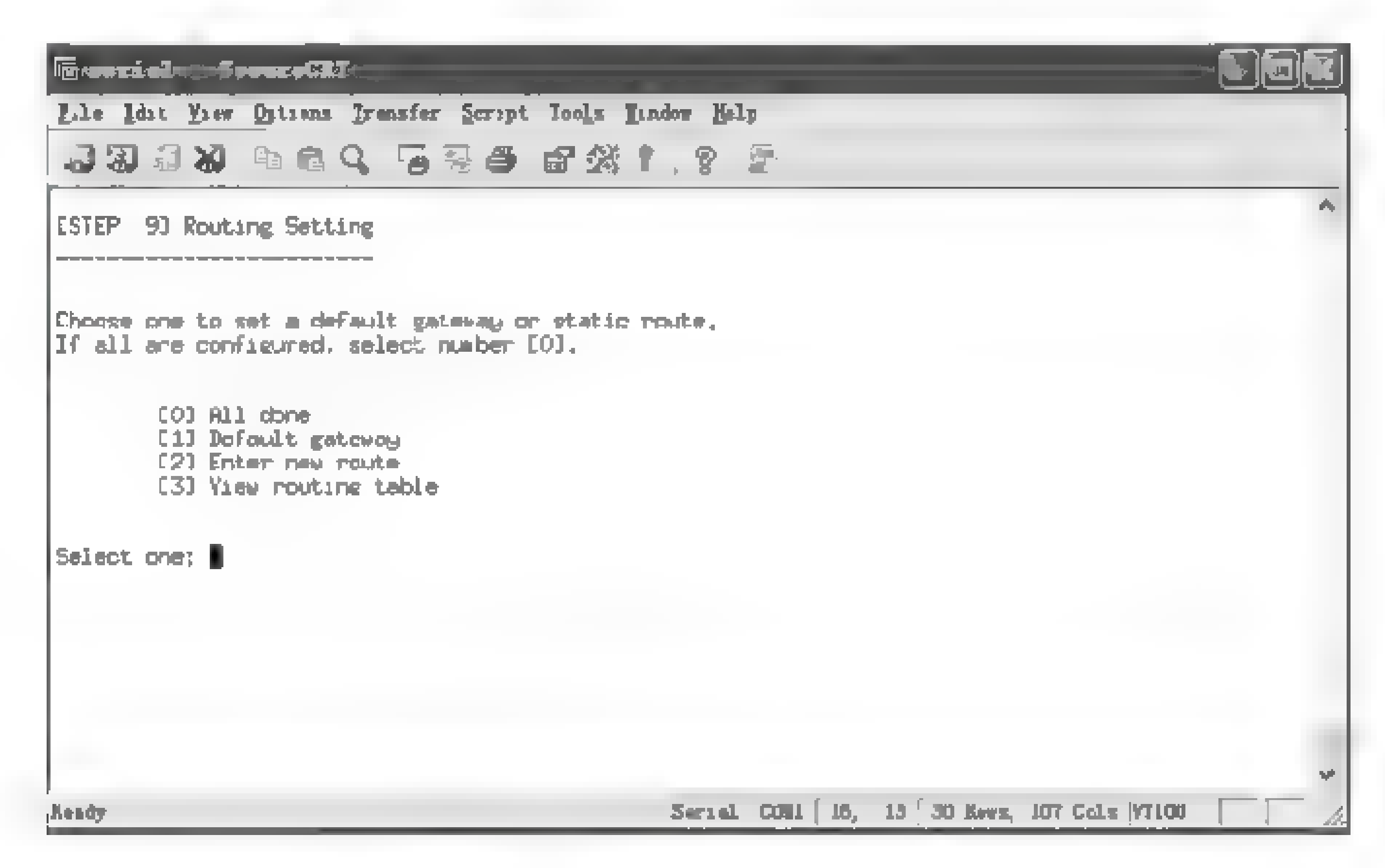


图 4-27 防火墙路由配置

10. 设置 OSPF

在路由模式下才可以设置 OSPF。如果没有必要启用 OSPF,选择[0]跳过,如图 4-28 所示。

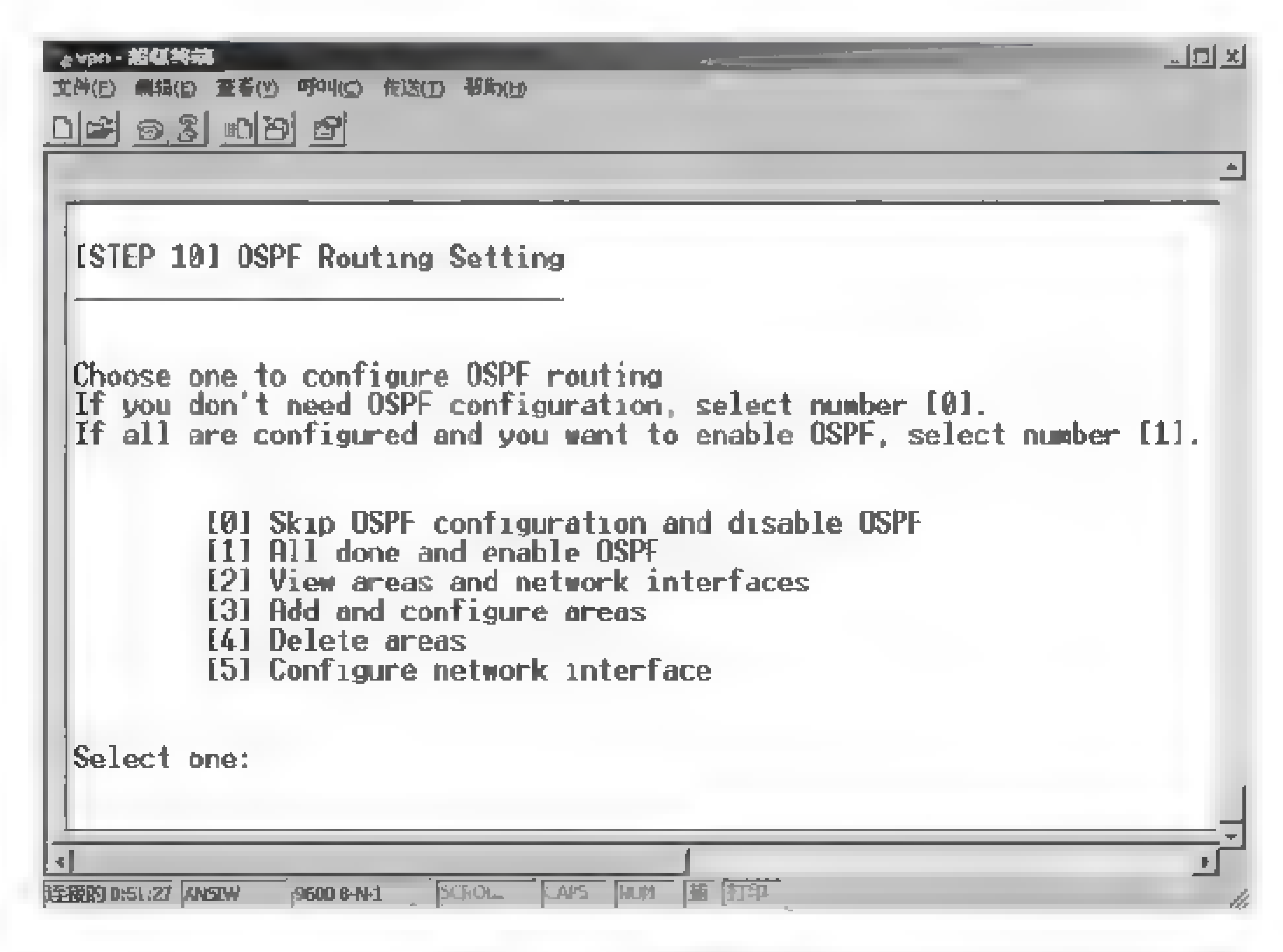


图 4-28 设置 OSPF

完成所有 OSPF 构成以后，选择[1]即可应用。

要构成 OSPF，首先设置 Area，假设设置 Area 为 2。当前 Area 以及接口的 OSPF 信息可以通过选择[2]来确认。

11. 设置 HA Zone

架设路由模式下高层可用结构时，首先要确定是否启用虚 IP 地址、配置什么样的虚 IP 地址，以及是否使用四层交换机来实现高层同步模式。

图 4-29 所示为 HA 构成的画面，在此输入组成 HA Zone 的 RG WALL 组名，默认值为 Default。

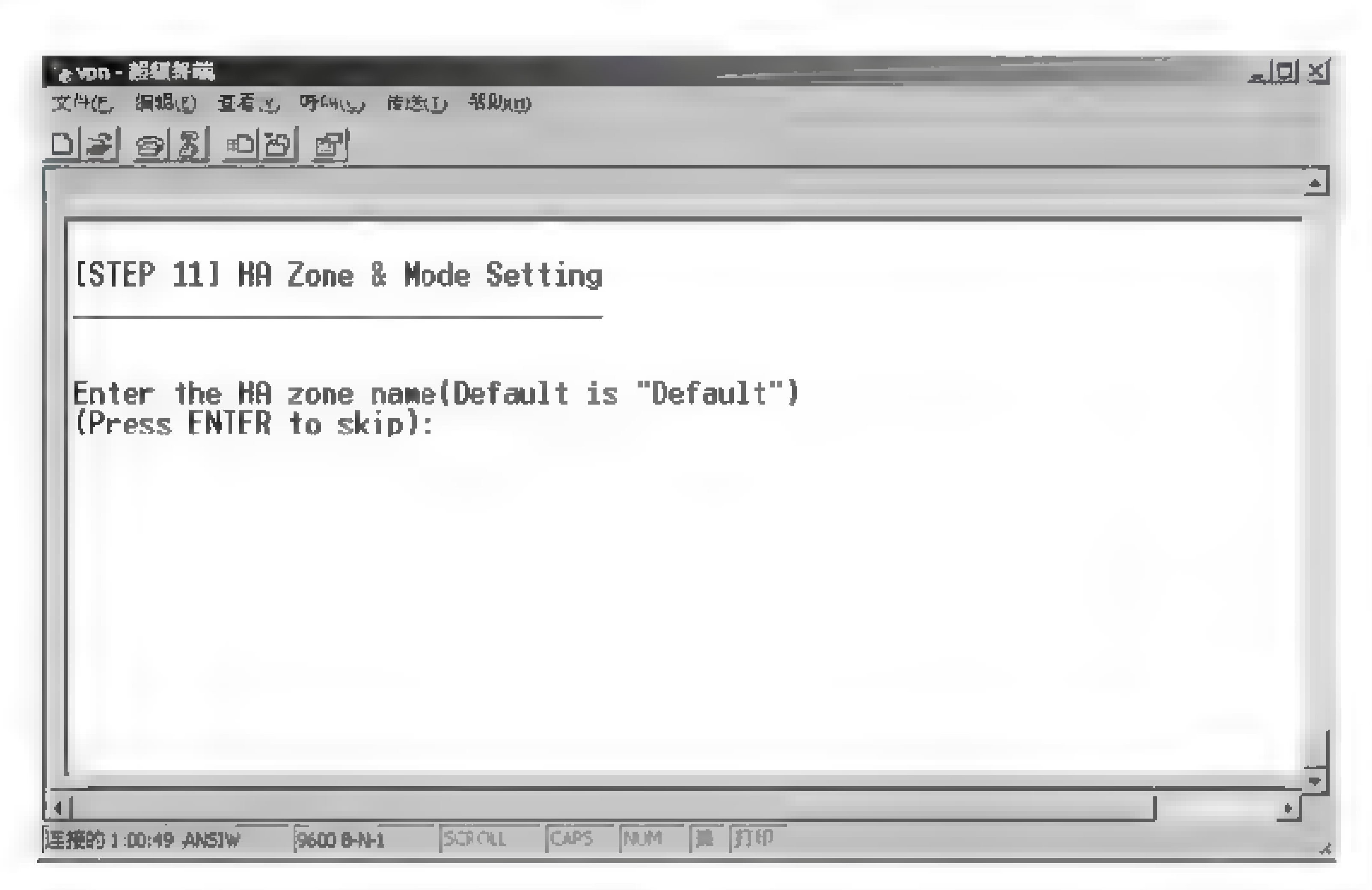


图 4-29　设置 HA Zone

12. 设置虚 IP 地址

图 4-30 所示是设置虚 IP 地址的阶段。首先要构成 VIG(Virtual Interface Group)，

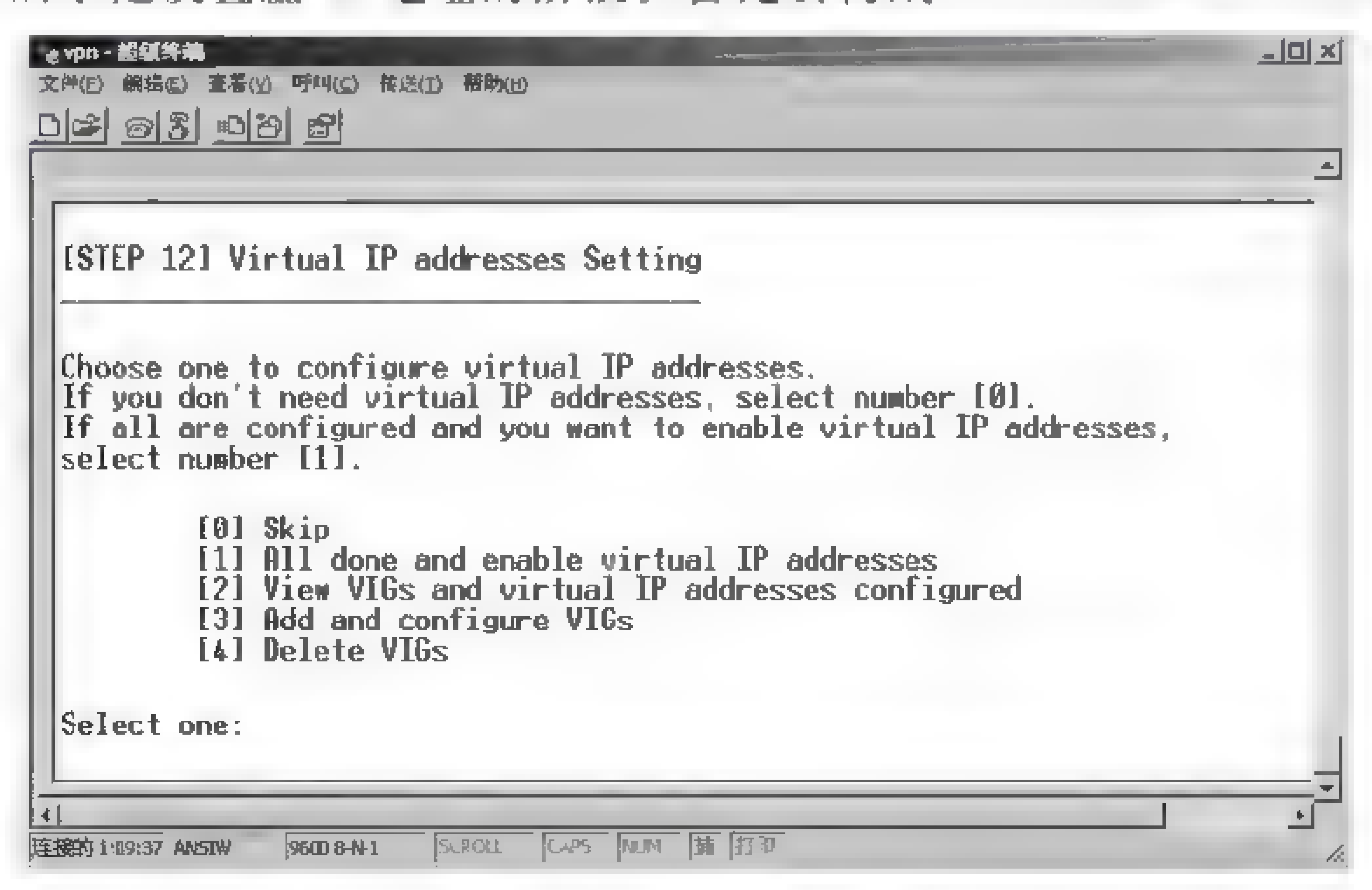


图 4-30　设置虚 IP 地址

选择[2],可以确认当前的 VIG,以及各接口的虚 IP 地址信息。

13. 设置 DNS

设置 DNS 输入域名,然后按 Enter 键,进入下一阶段,如图 4-31 所示。

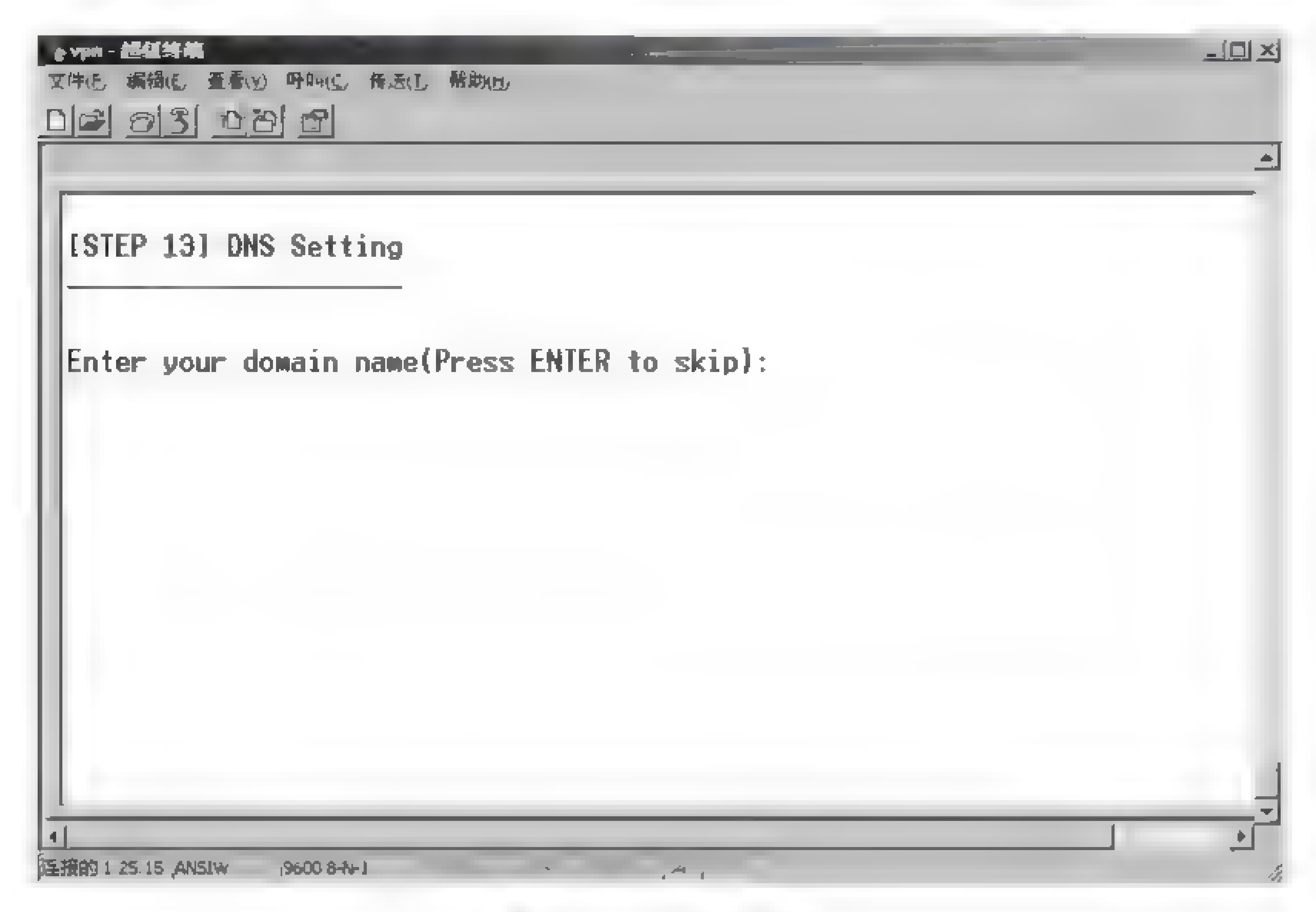


图 4-31　设置 DNS

14. 选择基本规则

最后一个阶段是设置初始规则,如图 4-32 所示。选择需要的基本规则即可,然后通过 GUI 进一步设置。

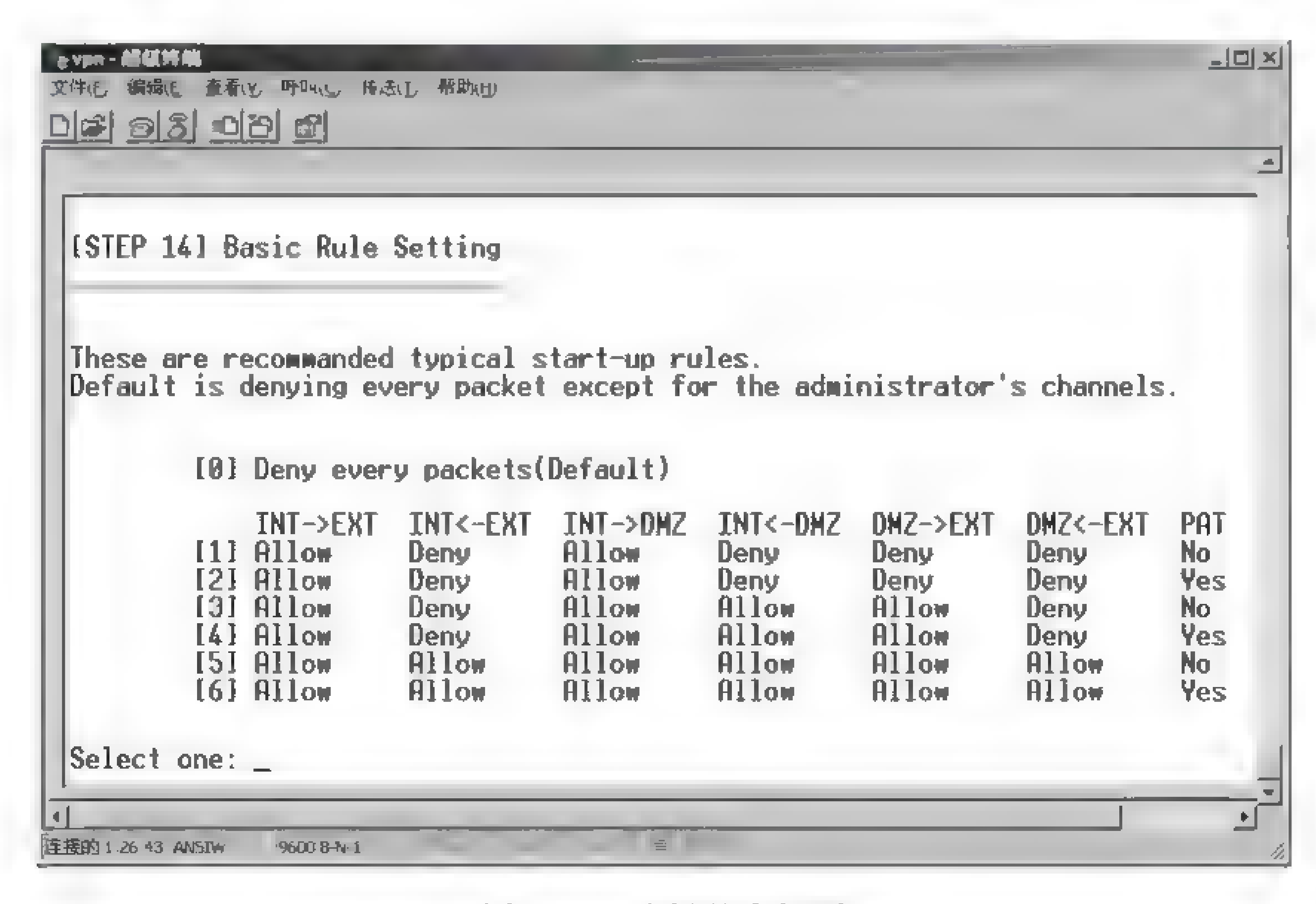


图 4-32　选择基本规则

15. 应用系统设置

基本安装设置完成后，出现如图 4-33 所示的安装完毕画面。按任意键重新启动系统，应用当前设置。

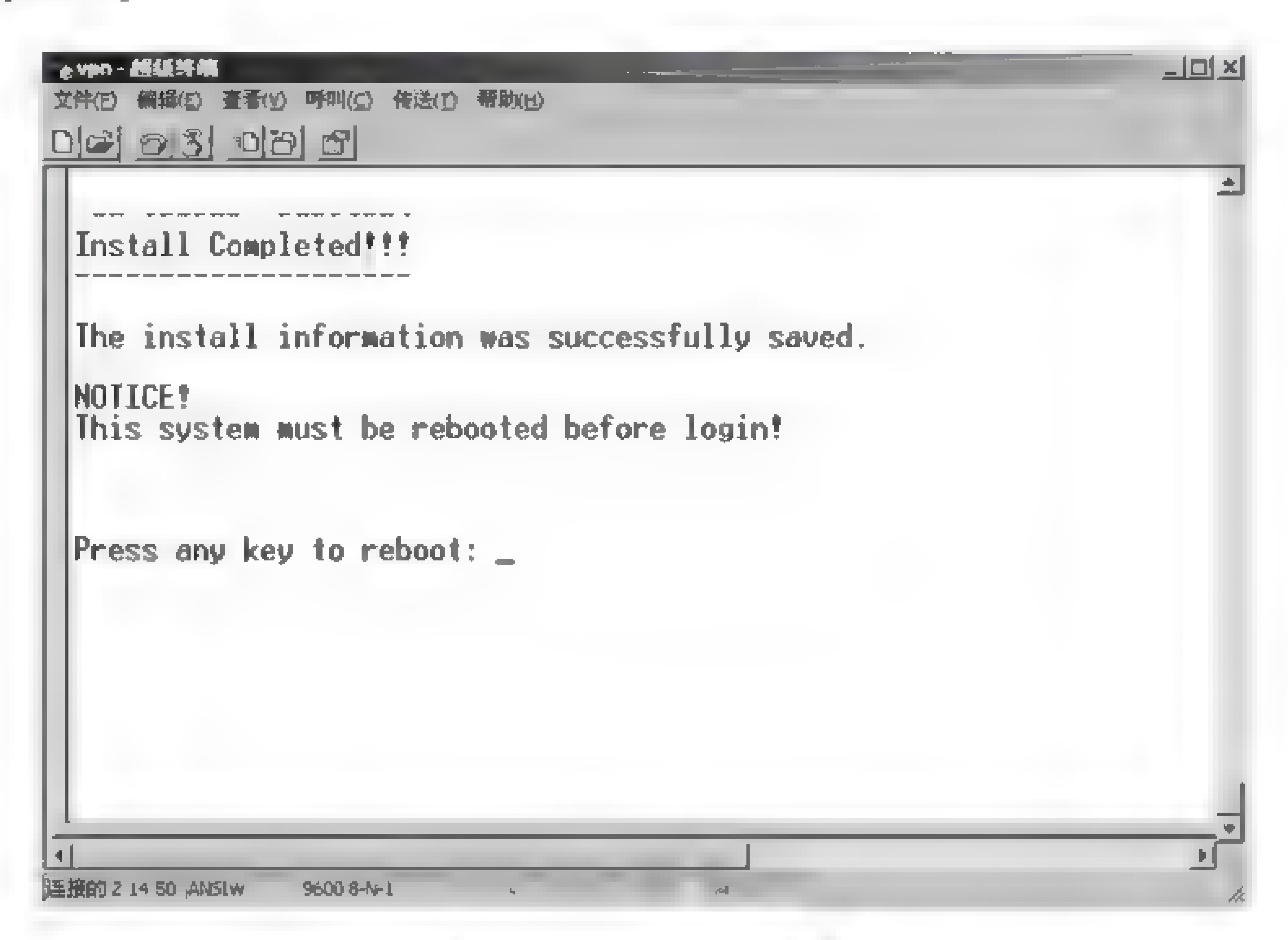


图 4-33　应用系统设置

重新启动后出现如图 4-34 所示画面，出现 RG-WALL 的登录提示符。登入 RG-WALL 系统后，将出现如图 4-35 所示 CLI 基本菜单。

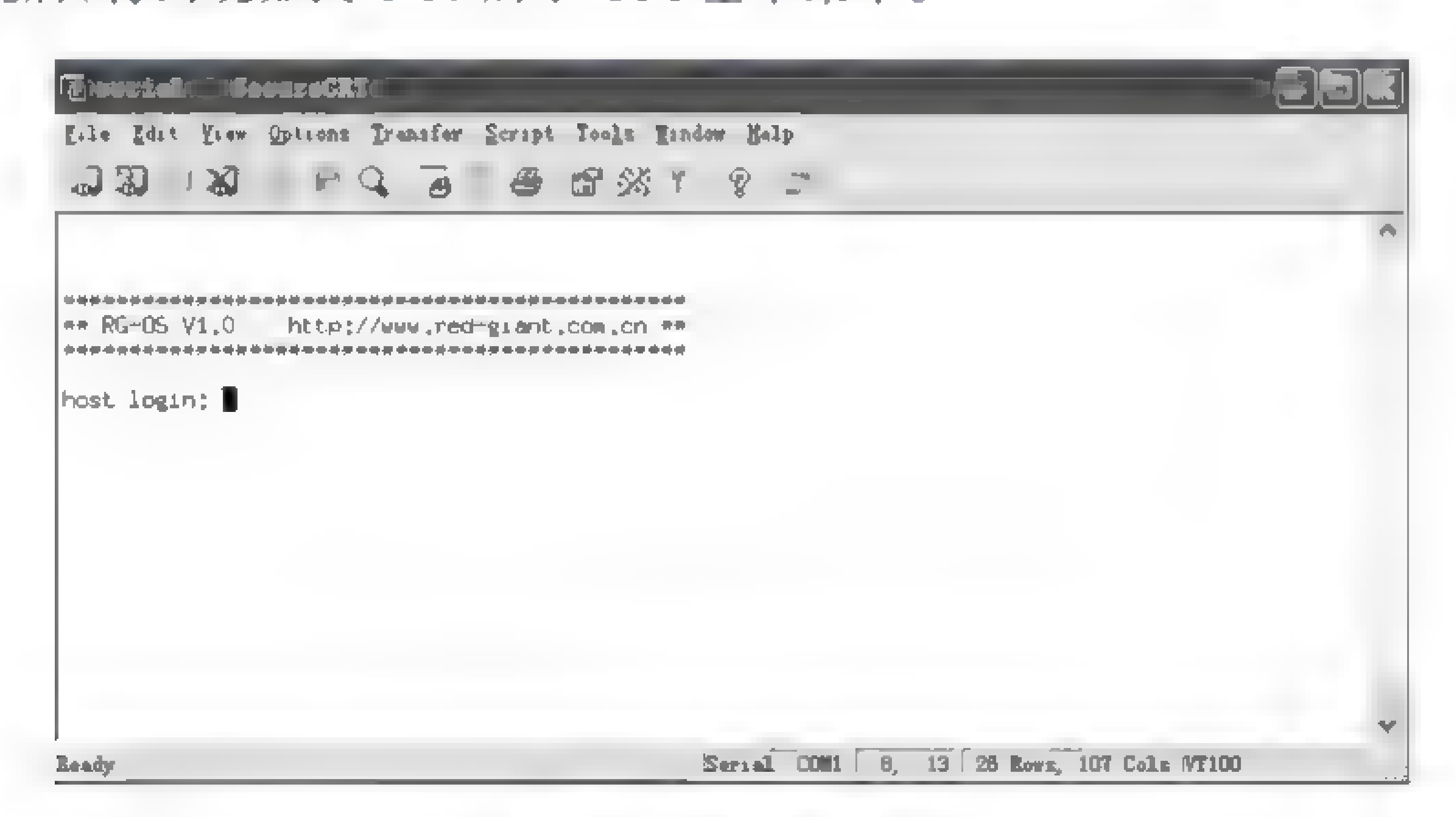


图 4-34　登录设置(1)

继续通过 CLI 执行操作，可以选择[2]或者[3]。CLI 的详细说明请参考管理员手册。

16. 重新安装

RG-WALL 的重新安装提供了路由模式设置和网桥模式设置中的所有项。

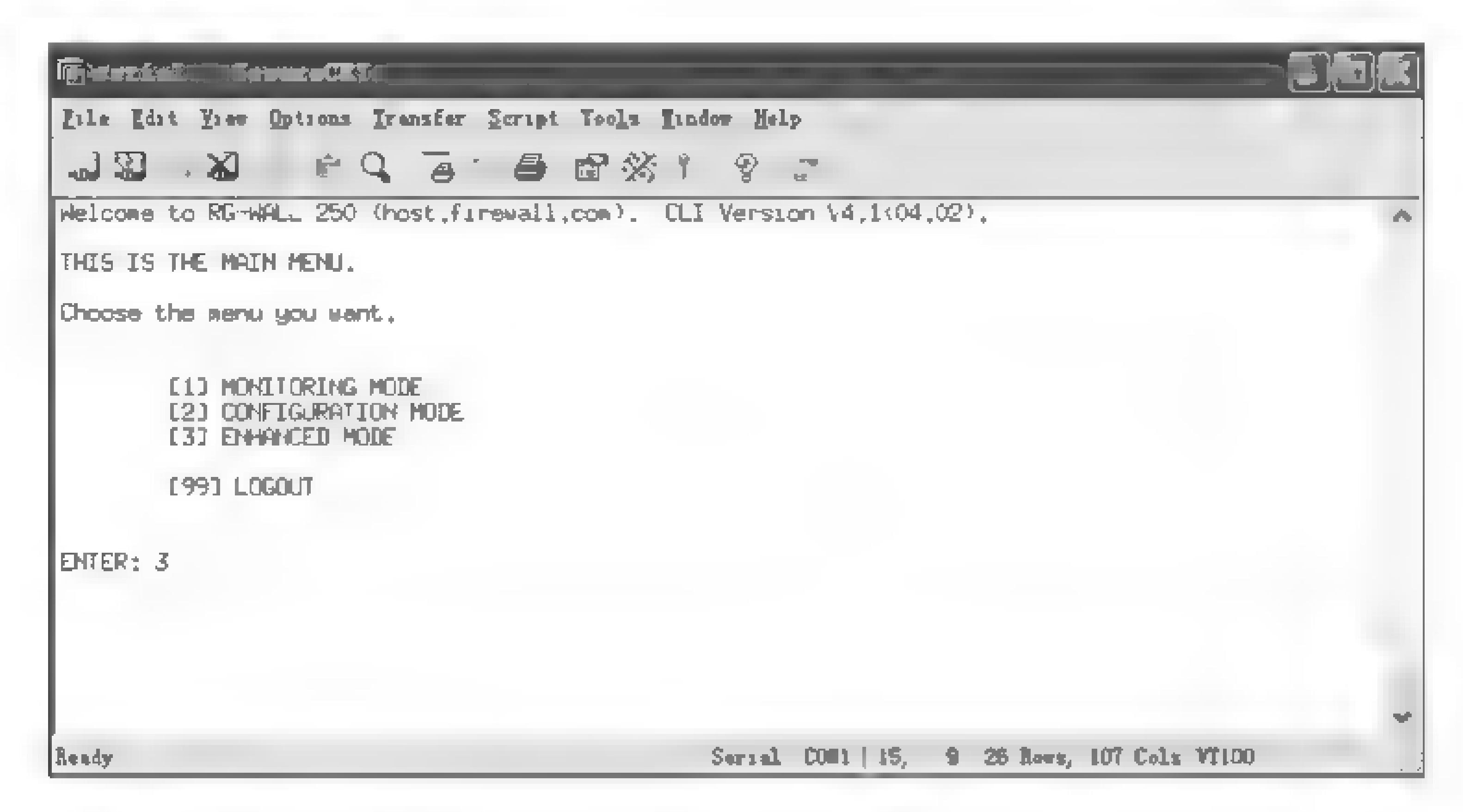


图 4-35 登录设置(2)

在 CLI 主菜单中选择[3],进入 CLI 的 ENHANCED MODE,可以重新设置 RG-WALL,如图 4-36 所示。在出现的 CLI ENHANCED MODE 画面中,在 CLI 命令提示符后输入“reinstall”,重新设置系统。

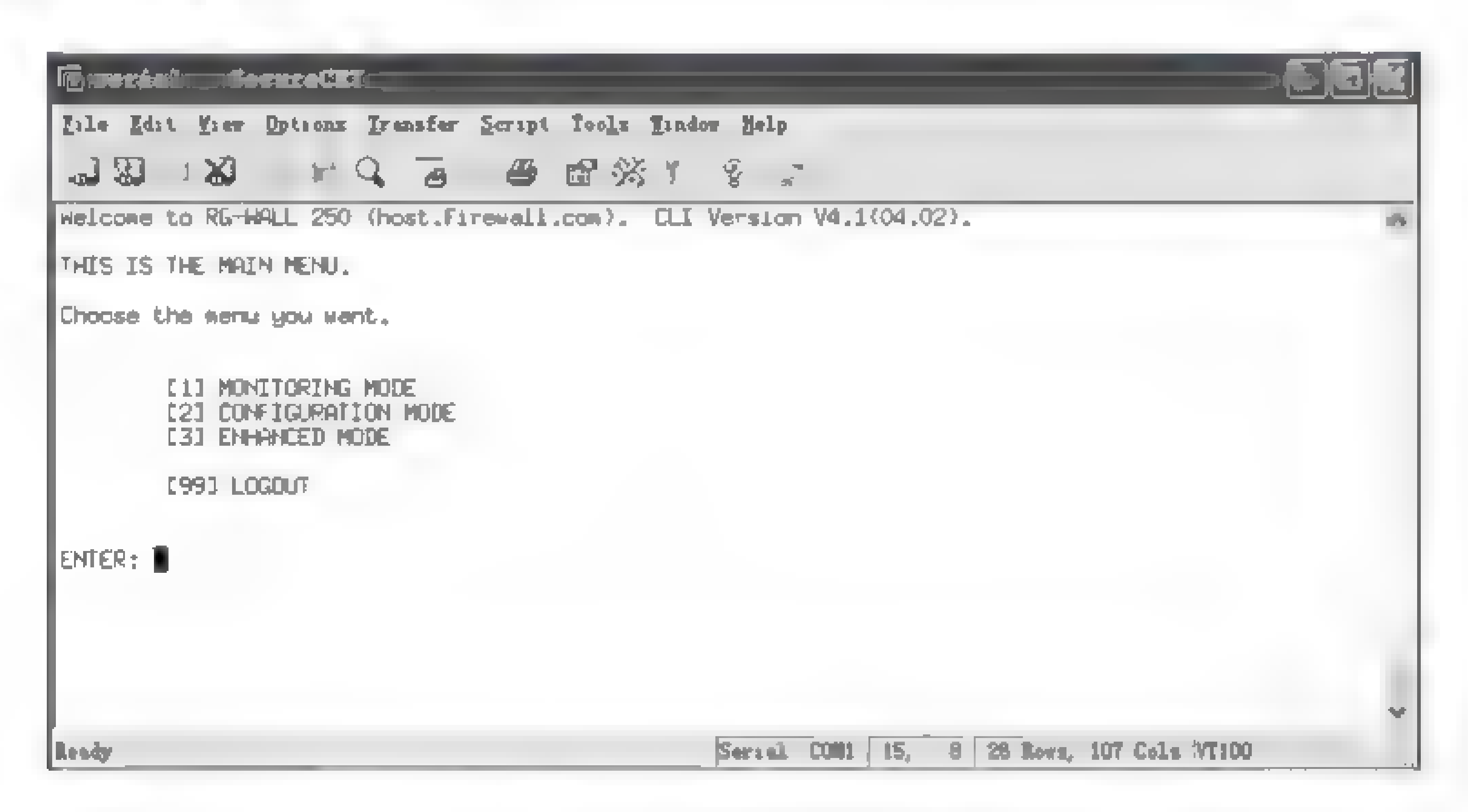


图 4-36 重新设置系统

17. GUI 安装

RG WALL 的 GUI 通过 Java 技术实现,因此兼具客户端软件管理方式和 Web 浏览器管理方式的优点。它支持多种语言,与管理工作站的操作系统无关。

为了运行 Java 类程序,管理员工作站需要具备 SUN 公司的免费软件 Java Runtime Environment (JRE)。在管理员工作站上启动 Web 浏览器后,在地址栏中输入 RG WALL Internal 接口的 IP 地址,出现图 4 37 所示的初始界面。RG WALL Desktop 画面如图 4-38 所示。

18. 确认安装是否正常

进入 RG-WALL CLI 模式并输入以下命令:

```
[admin:E:W] RG-WALL>ping"与各接口连接的对方设备 IP 地址"
```

连接防火墙的网络设备经过 ping 测试连通性成功以后，可以再 ping 测试管理员 PC、DMZ 内部的主要服务器以及外网常用的 IP 地址。



图 4-37　RG-WALL 初始界面



图 4 38　RG-WALL Desktop 画面

任务 4.4　建立外部安全数据通道——VPN

情境回顾：公司在全国各地都有办事机构，需要访问公司内部的服务器资源，而这些服务器资源出于安全性考虑不直接在公网上开放，因此必须建立 VPN 隧道，再获得访问内部资源的权利。下面以锐捷产品为例来介绍。

任务所需要的设备如表 4 8 所示，网络拓扑如图 4 39 所示。

表 4-8 建立 VPN 模型所需设备

设　　备	型　号	数　量	备　注
锐捷 VPN 设备	RG-WALL 150	1 台	
锐捷 VPN 远程接入系统	RG-SRA	1 套	软件程序
锐捷路由器设备		1 台	
Windows 系统的 PC 机	推荐 Win XP 系统	1 台	
Windows 系统的服务器		1 台	建议开设 FTP 服务或者 Web 服务
直连线		2 根	
交叉线		1 根	

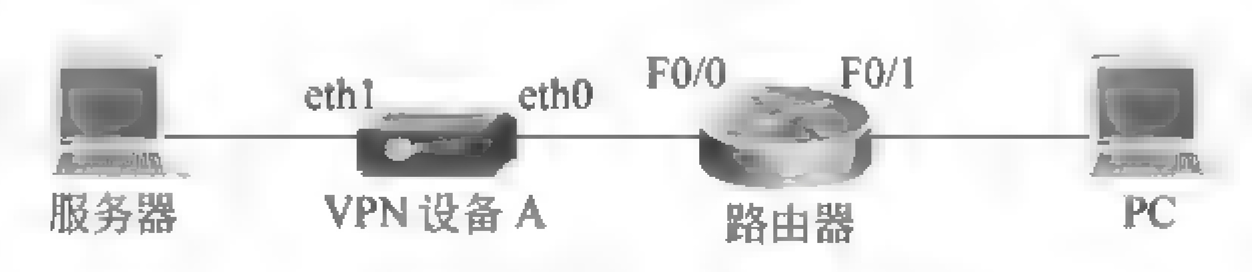


图 4-39　简单 VPN 网络拓扑图

1. 准备好 PC 机和服务器

实际操作中既可以通过 PC 机来管理 VPN 设备 A，也可以通过服务器来管理 VPN 设备 A，请自行选择。

假设决定用服务器来管理 VPN 设备 A，则在服务器上安装 VPN 管理软件(VPN 设备随机光盘)。

在 PC 机上安装 RG-SRA 软件程序，安装步骤请看随机附带的光盘，这里不再详述。

注意：*RG-SRA 是 VPN 客户端软件程序，如果 PC 机上已预装其他厂家的 VPN 客户端程序，请先卸载，否则 RG-SRA 可能无法正常工作。*

RG-SRA 作为安全产品，安装后对系统的网卡、端口、协议等方面有改动，会和部分防火墙或者防病毒程序不兼容。经过测试，已知和市场主流的杀毒软件、防火墙兼容的有瑞星、天网、Symantec、微软等产品，已知的不兼容的软件有卡巴司基、Sygate。因此建议用于测试的 PC 机卸载这两个程序。推荐用户使用没有安装任何第三方防火墙、防病毒程序的机器来进行操作。

2. 搭建拓扑

配置 PC 机、服务器、VPN 设备 A、路由器的 IP 地址及必要路由。示例如下：

VPN 设备 A 的 eth1 口地址：192.168.2.1

VPN 设备 A 的 eth0 口地址：10.1.1.1

PC 机的 IP 地址：10.1.2.1

PC 机的网关地址：10.1.2.2

服务器的 IP 地址：192.168.2.2

服务器的网关地址：192.168.2.1

路由器的 F0/0 地址：10.1.1.2

路由器的 F0/1 地址：10.1.2.2

注意：PC 机及路由器的详细配置省略，请参考相关操作手册。

RG-WALL 150 设备接口标识为“WAN”口，对应系统内部显示为“eth1”的接口；接口标识为“LAN”口，对应系统内部显示为“eth0”的接口。

VPN 设备 A 接口及默认路由配置如下：

(1) 通过服务器的超级终端，在命令行下配置 VPN 设备 A 的 eth1 口地址，如图 4-40 所示。

```
RG-WALL login: sadm
Password:
[sadm@RG-WALL]# network
[sadm@RG-WALL(Network)]# interface set
Interface to set (eth0, eth1, Enter means cancel):
eth1
Bring up onboot? (0: No, 1: Yes, Enter means Yes)
1
Work mode (0: UnCfg, 1: Manual, 2: DHCP, 3: PPPoE, 4: InBridge, Enter means Manual):
1
IP Address (xxx.xxx.xxx.xxx):
192.168.2.1
Netmask (xxx.xxx.xxx.xxx, Enter means 255.255.255.0):
255.255.255.0
GateWay (xxx.xxx.xxx.xxx, Enter means no default gateway in this network):

MAC Address (xx:xx:xx:xx:xx:xx, Enter means use MAC Address of device):

MTU (68-1500, Enter means use MTU of device):

[sadm@RG-WALL(Network)]#
```

图 4-40　配置 VPN 设备 A 的 eth1 地址

注意：锐捷 VPN 出厂时，eth1 口默认地址为 192.168.1.1。

(2) 通过服务器上的 VPN 管理软件登录 VPN 设备 A，然后配置 eth0 口地址，如图 4-41 所示。设置 eth0 口地址的界面如图 4-42 所示。

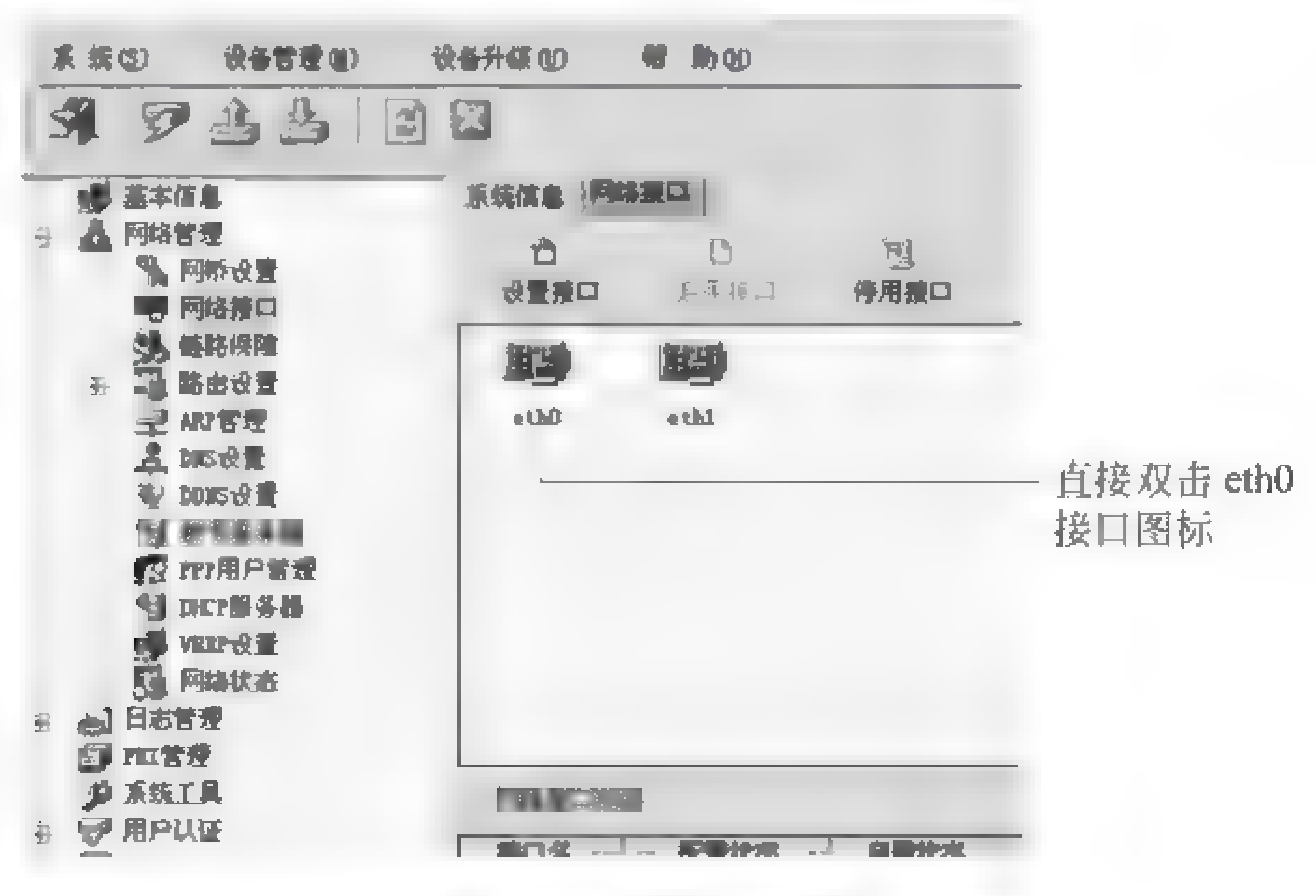


图 4-41　配置 eth0 地址

验证测试：

① VPN 设备 A 可以 Ping 通路由器的 F0/0 口；

② PC 机可以 Ping 通路由器的 F0/1 口；

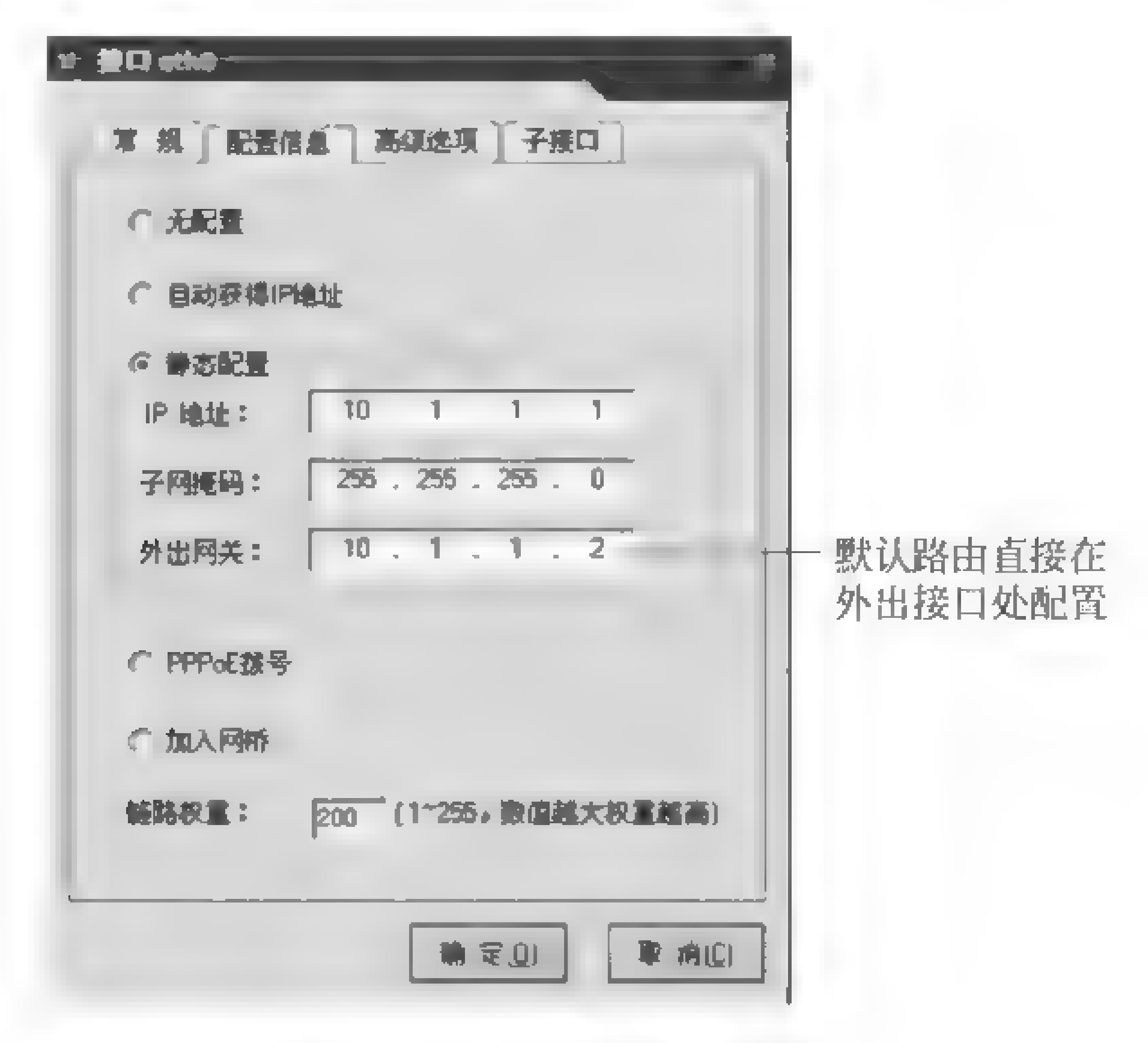


图 4-42　设置 eth0 地址

③ PC 机可以 Ping 通 VPN 设备 A 的 eth0 口；

④ 服务器可以 Ping 通 VPN 设备 A 的 eth1 口。

3. 配置 IPSec VPN 隧道

(1) 在 VPN 设备 A 上进行 IPSec VPN 隧道配置。

① 进入远程移动用户 VPN 隧道配置的界面。登录 VPN 设备 A 的管理界面，选择进入“远程用户管理”界面，如图 4-43 所示。

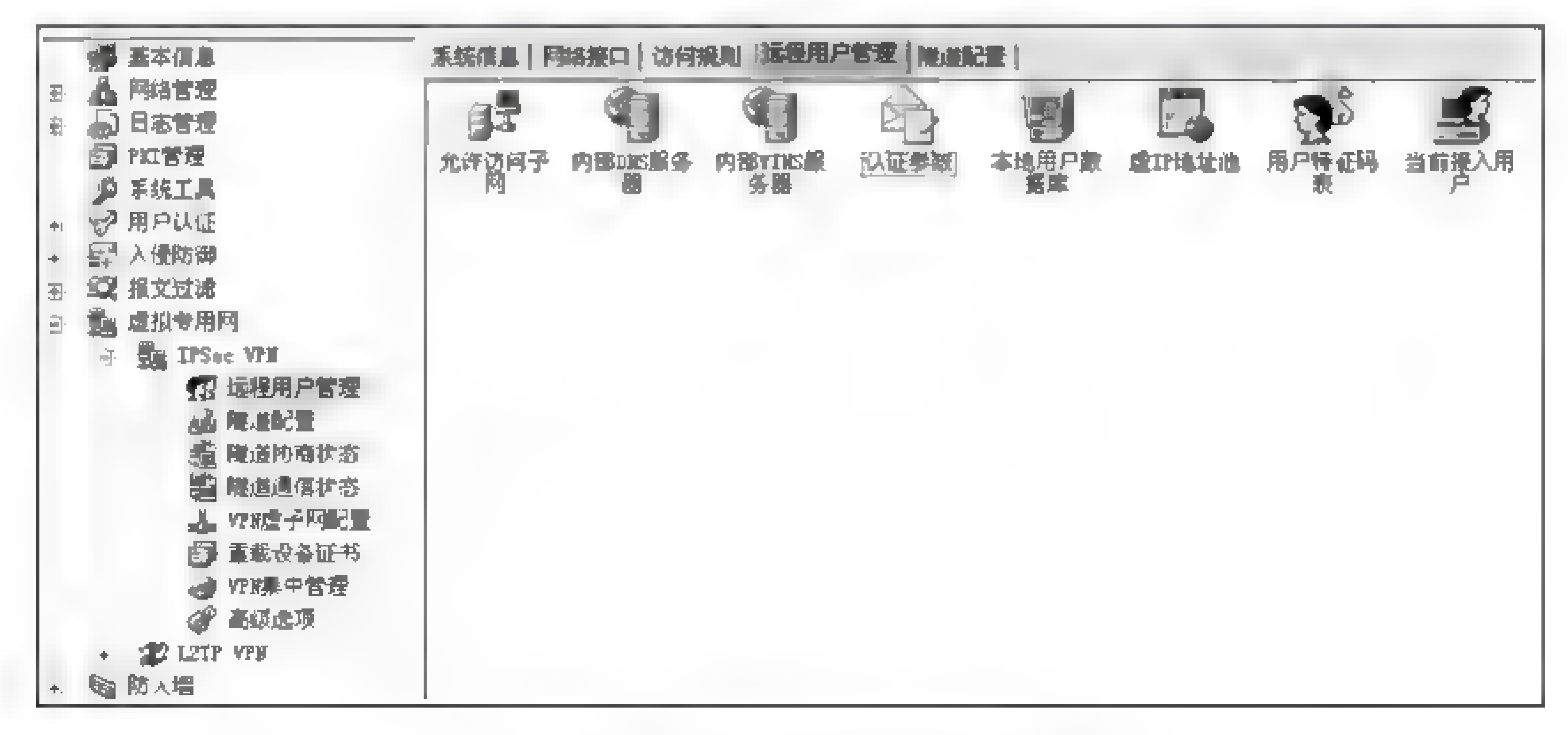


图 4-43　“远程用户管理”界面

② 配置“允许访问子网”，如图 4-44 所示。

③ 配置“本地用户数据库”，如图 4-45～图 4-48 所示。

注意：添加完用户后一定要单击“用户生效”按钮，否则新添加的用户不可用。

④ 配置“虚 IP 地址池”，如图 4-49 所示。

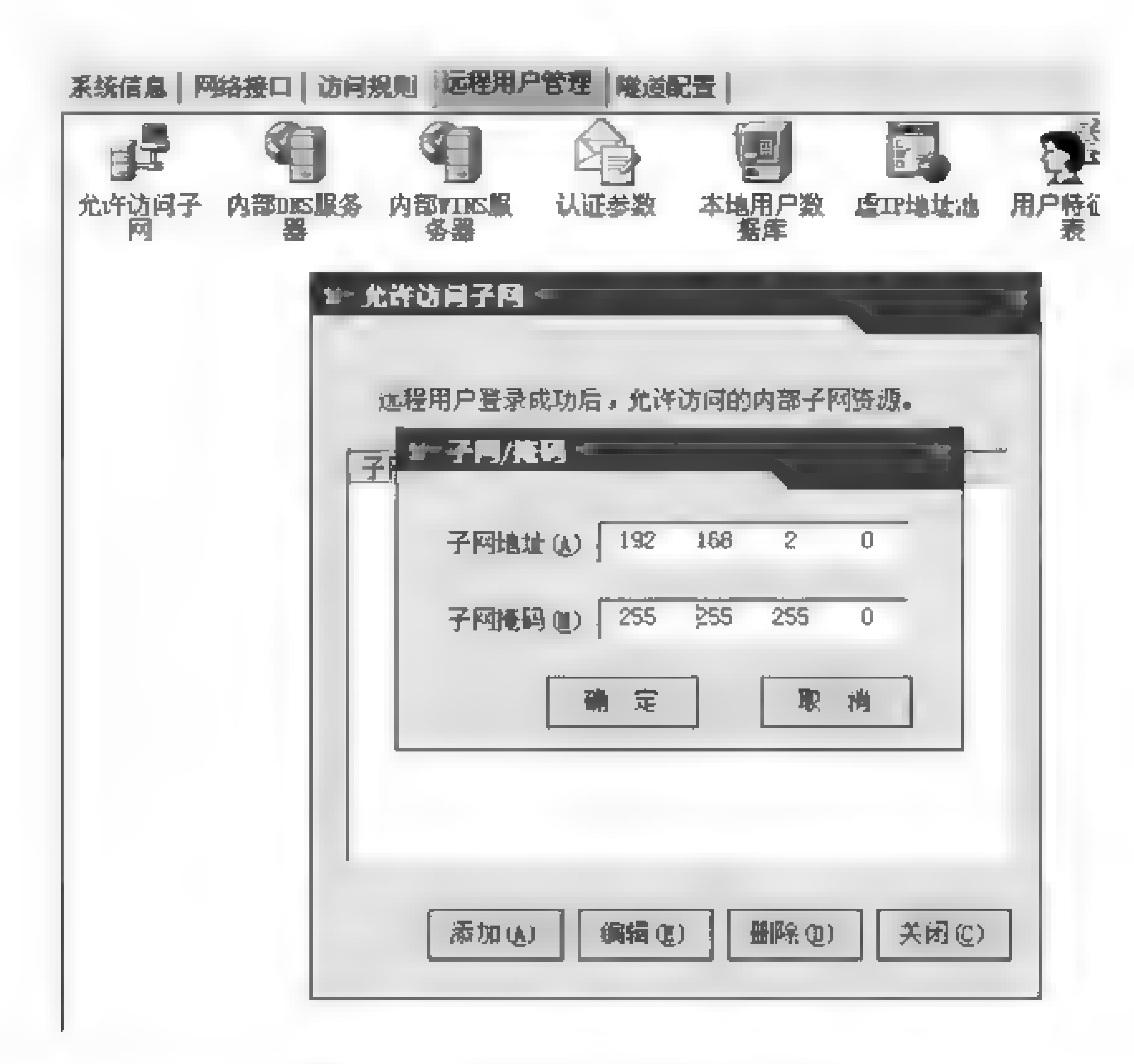


图 4-44　配置"允许访问子网"



图 4-45　配置本地用户数据库(1)

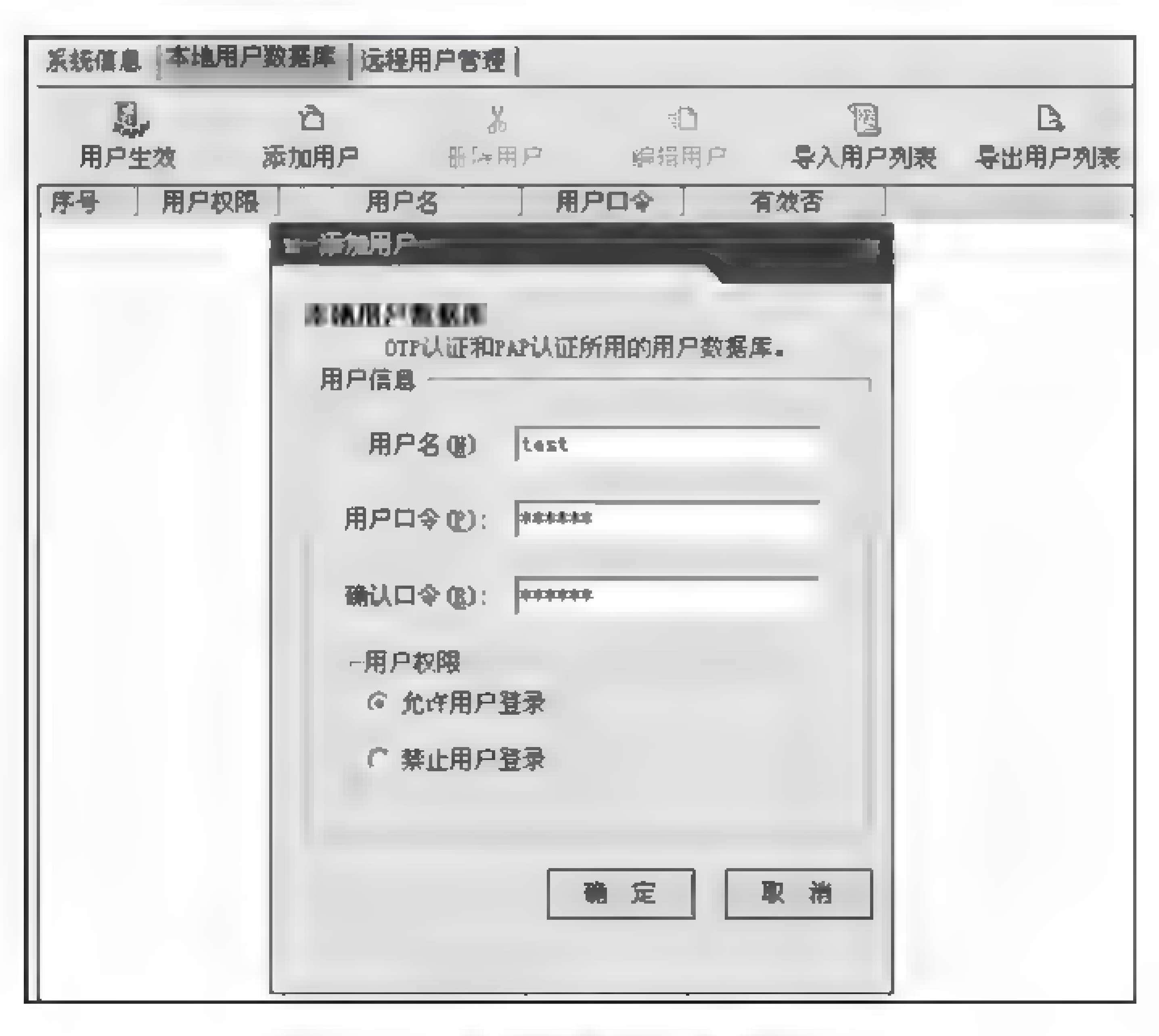


图 4-46　配置本地用户数据库(2)



图 4-47　配置本地用户数据库(3)

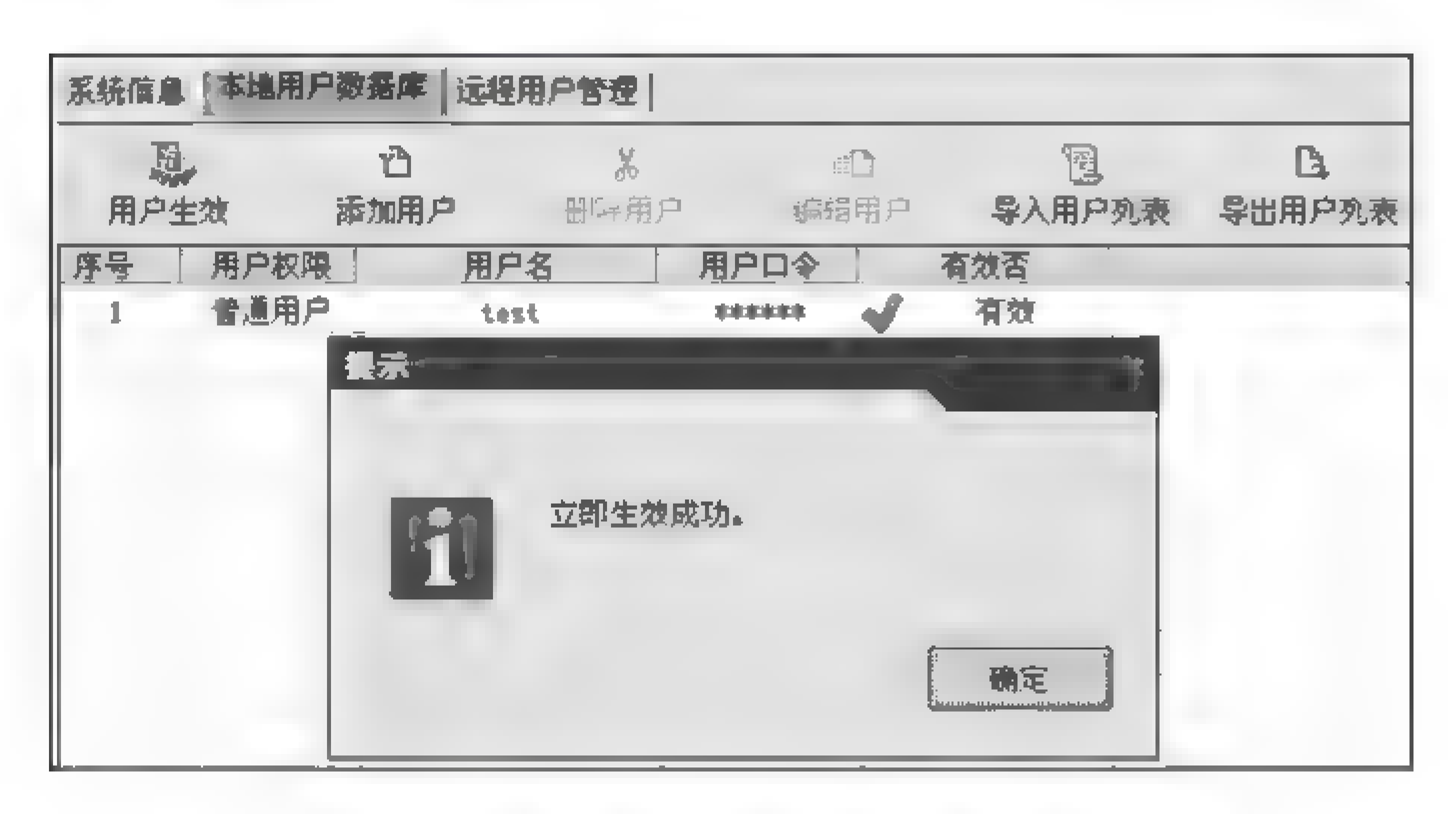


图 4-48　普遍用户设置生效

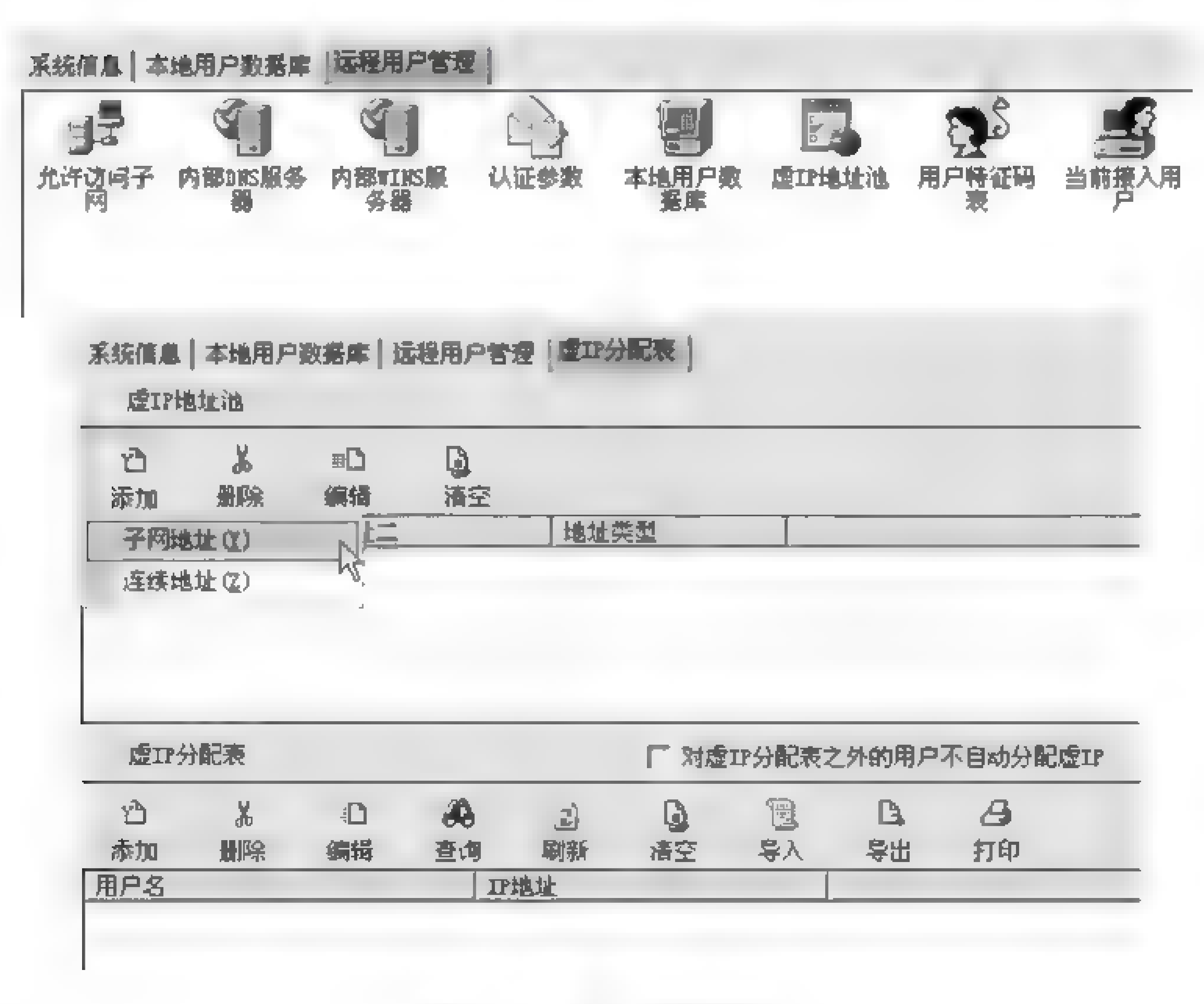


图 4 49　虚 IP 地址池

注意：分配 PC 机的虚拟 IP 地址，既可以是定义一个地址池，由 VPN 设备自动分配；也可以是管理员一个 IP 地址对应一个用户地分配。在这里选择地址池方式，由系统自动分配，并且选择定义“子网地址”的地址池。

虚拟 IP 地址是网络管理员分配给远程移动用户的，表示只有拥有该地址的 PC 机才

能获得局域网内部的访问权限。因此，管理员设置的虚拟 IP 地址一定不要与远程 PC 的 IP 地址以及局域网内部的 IP 地址相冲突，否则远程 PC 在和 VPN 设备建立隧道后，因地址冲突的问题，将无法访问局域网内部的服务器。本项目中的虚拟 IP 地址池选择定义一个完全没有使用的网段，如图 4-50 和图 4-51 所示。

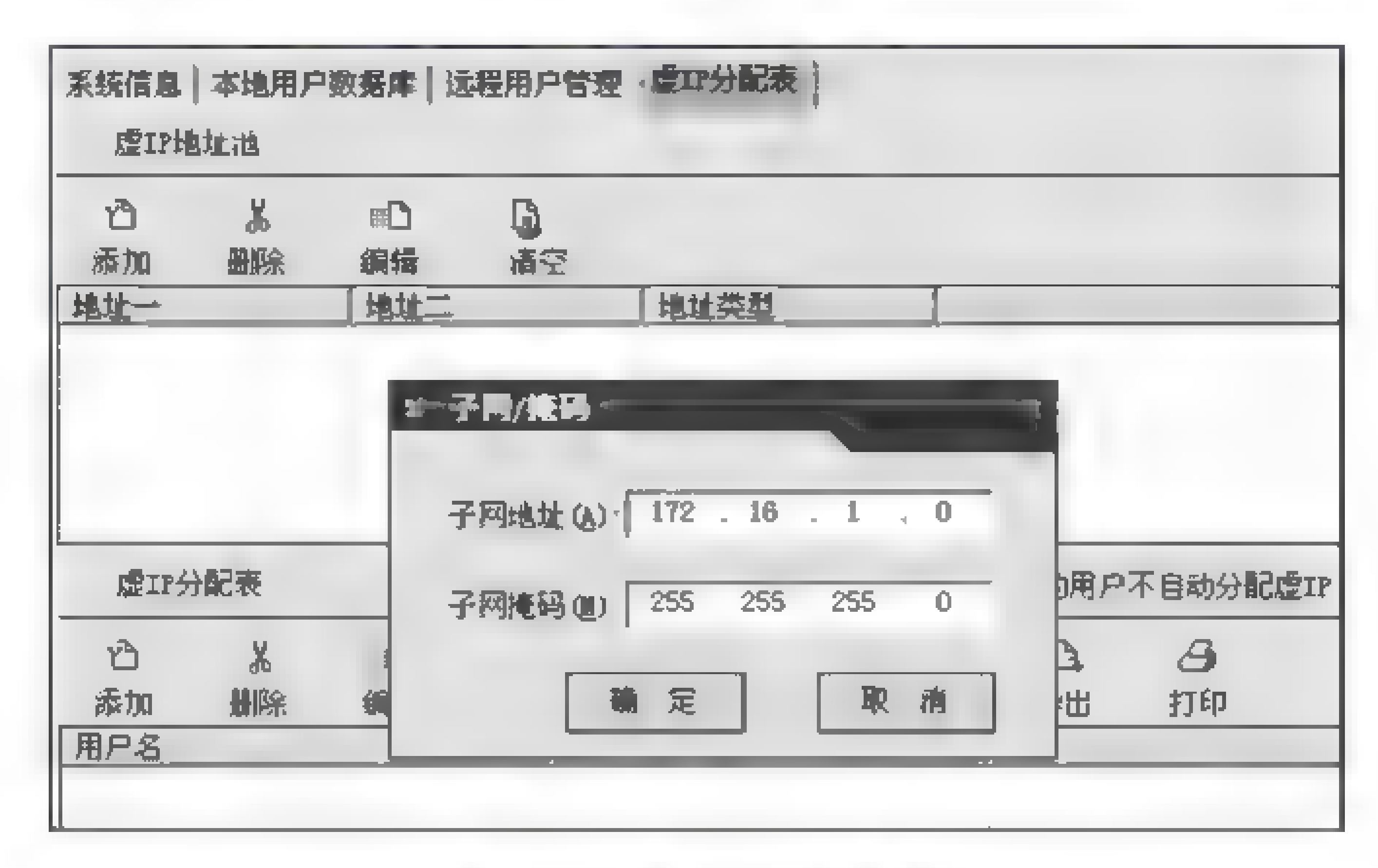


图 4-50　虚 IP 分配设置



图 4-51　虚 IP 分配成功

⑤ 配置“用户特征码表”，如图 4-52 和图 4-53 所示。

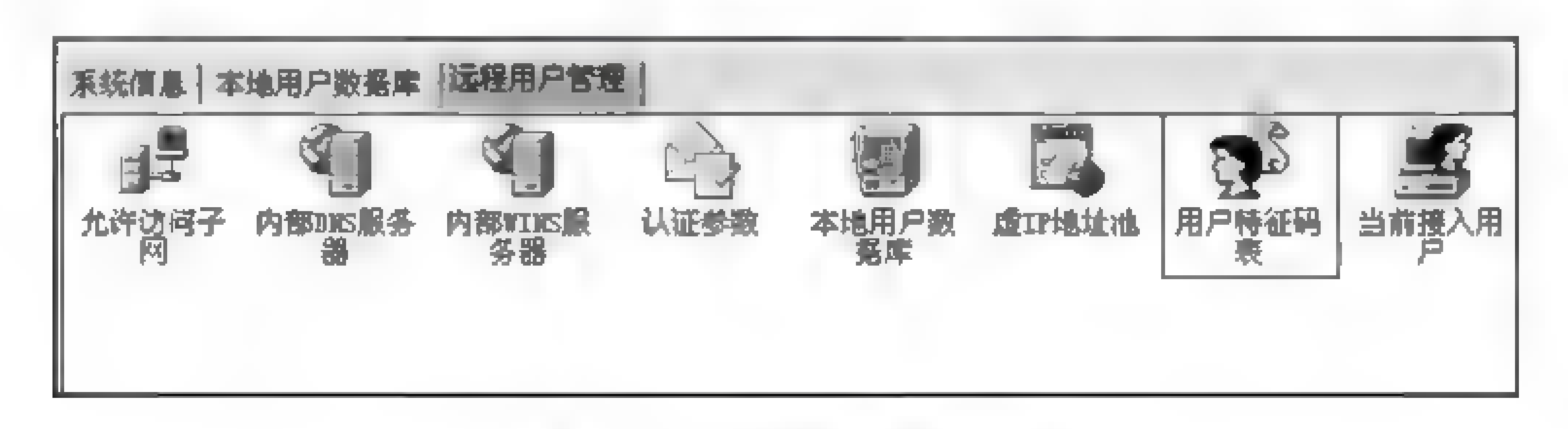


图 4-52　用户特征码表

“用户特征码表”是为了将远程 PC 的硬件和分配给用户的身份信息绑定而设计的。选择了“允许接入并自动绑定”功能，VPN 设备会将远程用户的 PC 硬件特征码与该用户的身份认证信息相绑定。绑定后，该用户将无法用自己的身份信息再在其他 PC 设备上建立 VPN 隧道。

本项目操作中既可以选择“允许接入”，也可以选择“允许接入并自动绑定”。系统默认配置是“禁止接入”。图 4-53 中选择的是“允许接入”，表示该用户的身份信息不会和其使用的 PC 硬件绑定。

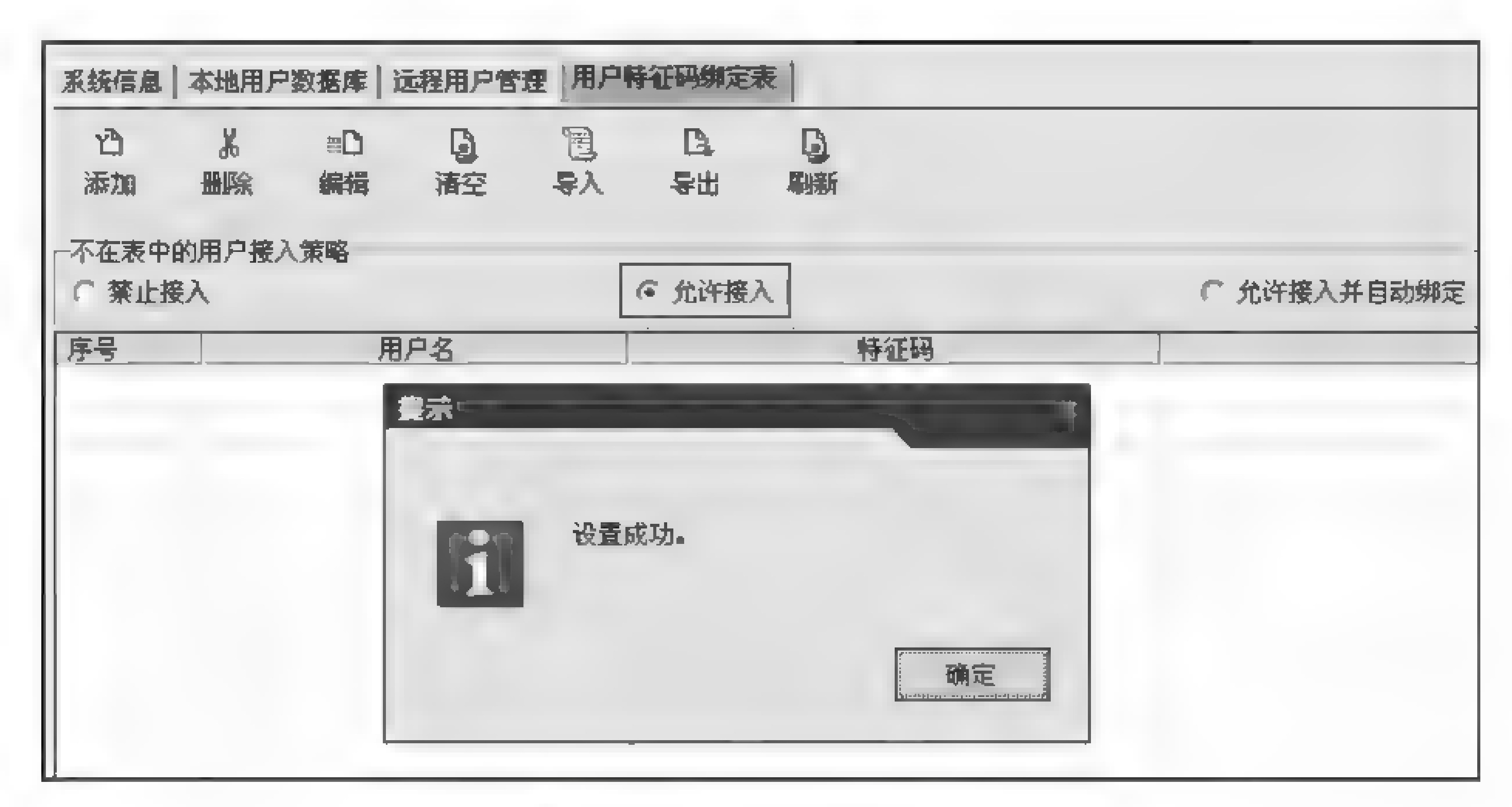


图 4-53　用户特征码绑定表

对于“远程用户管理”界面的其他配置项，例如“内部 DNS 服务器”、“内部 WINS 服务器”、“认证参数”，用户可以根据实际需要选择设置。

(2) 在 PC 机上运行 RG-SRA 程序，开始建立 VPN 隧道。

① 第一次运行 RG-SRA 程序后出现，如图 4-54 所示的界面。



图 4-54　SRA 界面

② 建立一个与 VPN 设备 A 的隧道连接。单击“新建连接”按钮，出现如图 4-55 所示界面；填写基本信息，如图 4-56 所示；单击“确定”按钮，如图 4-57 所示。

③ 运行该隧道连接，建立 VPN 隧道，如图 4-58 所示。输入身份认证所必需的账号，即在 VPN 设备 A 上添加的用户，如图 4-59 所示。单击“连接”按钮后，系统自动进行身份认证，并且开始 IKE 的协商，如图 4-60 所示。



图 4-55　VPN 配置



图 4-56　VPNA 隧道配置(1)



图 4-57　VPNA 隧道配置(2)



图 4-58 VPNA 隧道配置(3)



图 4-59 VPN 连接设置



图 4 60 VPN 连接过程

完成身份认证和隧道建立的操作后，RG SRA 程序会自动缩小图标显示在屏幕的右下角，如图 4 61 所示。

验证测试：

① 右击 RG-SRA 图标，在弹出的快捷菜单中选择“详细配置”命令，可以查看到隧道信息，如图 4-62 和图 4-63 所示。

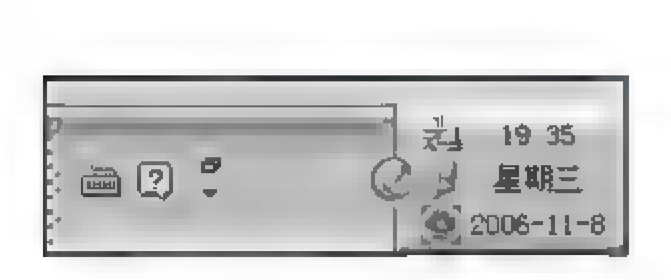


图 4-61 VPN 连接成功



图 4-62 VPN 查看信息



图 4-63 VPN 配置详细信息

② 在 VPN 设备 A 的管理界面也可看到已经建立成功的隧道信息。隧道启动后，可以在“隧道协商状态”栏目下看到隧道的协商状态，“隧道状态”显示“第二阶段协商成功”，如图 4-64 和图 4-65 所示。

图 4 64 隧道协商状态(1)

4. 进行隧道通信

从 PC 机访问服务器提供的服务，服务应该成功；或者先在 PC 机上 Ping 一下服务器的 IP 地址，应该能够 Ping 通(没有 VPN 隧道前，不会 Ping 通的)。

VPN 隧道的通信情况可以在“隧道通信状态”中查看到，如图 4-66 所示。

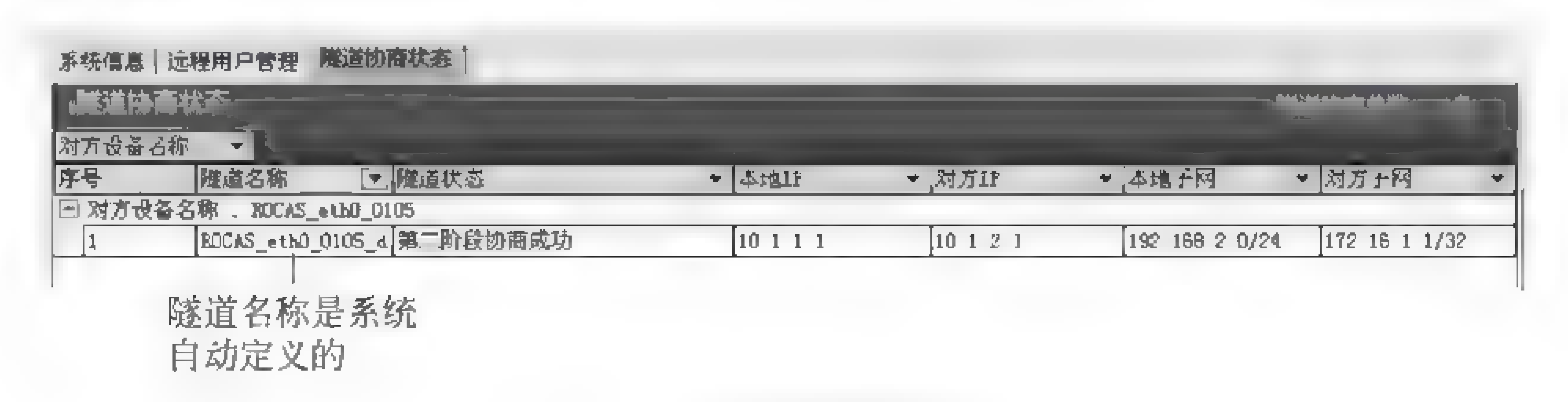


图 4-65 隧道协商状态(2)

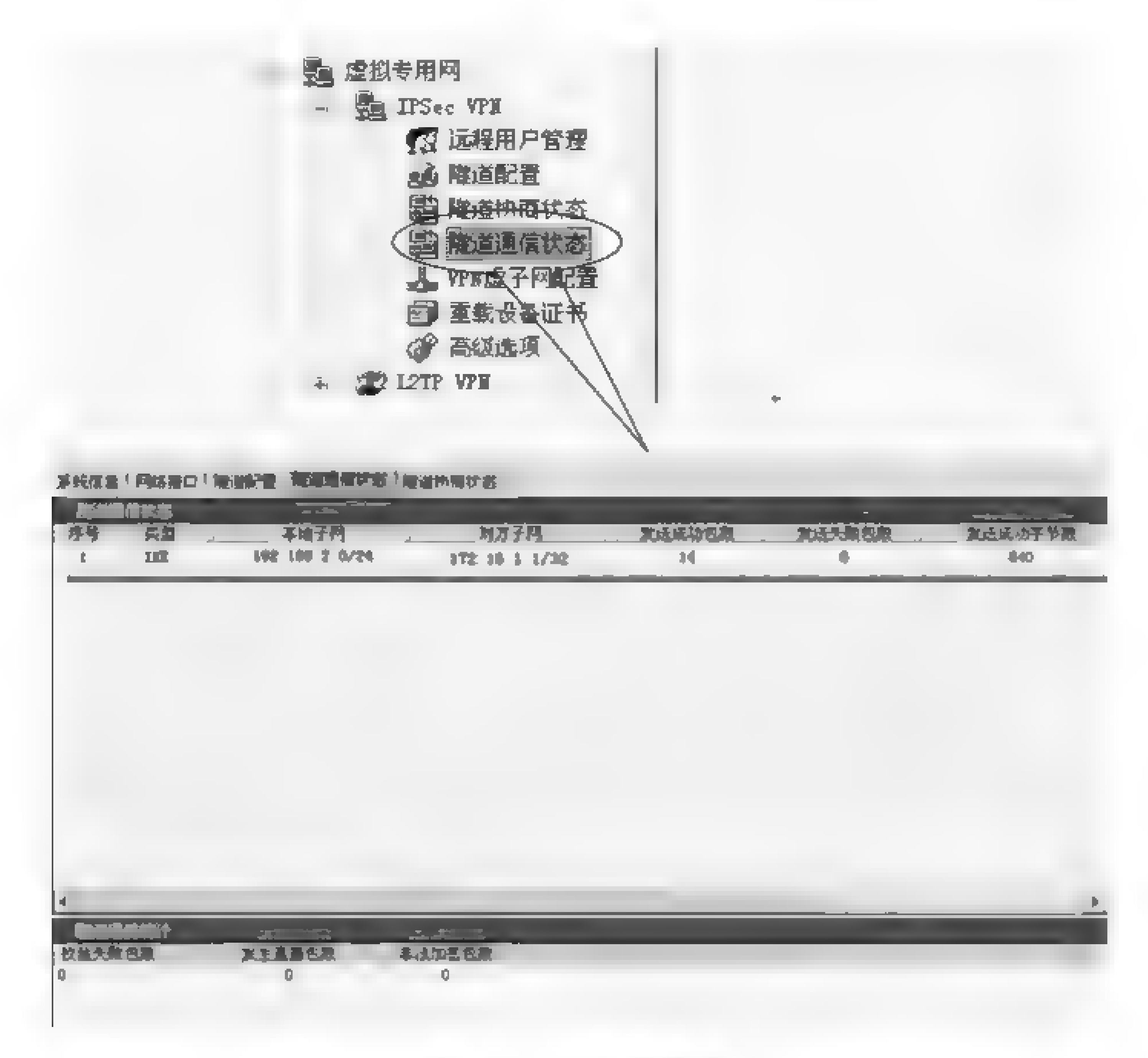


图 4-66　隧道通信

规律总结(检查)

ACL 访问控制列表的网络掩码是反掩码。标准控制列表要应用在尽量靠近目的地址的端口上。

在配置防火墙的初始配置中,关键是要设置管理员 ID、密码和 IP 地址,并设置至少一个接口的 IP 地址,其余配置可以在进入 Web 配置界面后设置。

VPN 配置 IP 地址可以随意定义,但请不要使用 1.1.1.0 这个网段的,因为某些功能实现的需要,VPN 系统内部已占用该网段的部分 IP 地址。VPN 设备的防火墙规则为全部开放。但在实际的网络环境中,如果 VPN 设备直接连接 Internet 网络,则一定需要启用防火墙规则。

拓展提高(拓展)

802.1 认证

鉴于公司网络安全管理的需要,需要对接入公司网络的用户进行必要的身份控制,公司决定部署基于 IEEE、802.1x 与 RADIUS 协议的认证管理系统。

任务所需设备：RG S2126G 一台;PC 机一台,用于配置交换机的终端。网络拓扑如图 4-67 所示。

操作过程如下:

第一步:查看交换机的版本信息。

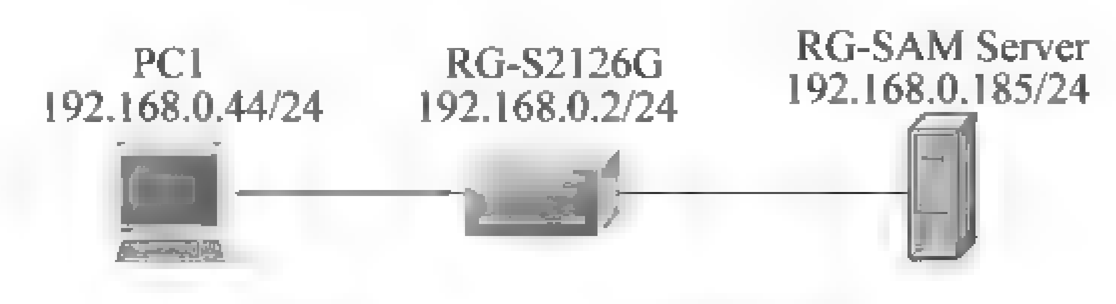


图 4 67　802.1 认证拓扑图

```
Switch> show version
System description       : Red-Giant Gigabit Intelligent Switch(S2126G) By Ruijie Network
System uptime            : 0d:0h:8m:40s
System hardware version : 3.3
System software version : 1.5(1) Build Mar 3 2005 Temp
System BOOT version      : RG-S2126G-BOOT 03-02-02
System CTRL version      : RG-S2126G-CTRL 03-05-02
Running Switching Image : Layer2
Switch>
```

第二步：初始化交换机配置。

所有的交换机在配置以前，必须先初始化，清除原有的一切配置，命令如下：

```
Switch>
Switch> enable
Switch# delete flash:config.text                  !删除配置
Switch# reload
…
Switch# configure terminal                        !进入配置层
Switch(config)#
```

验证测试：使用命令 show running-config 查看配置信息，删除原始配置信息后，该命令的打印结果如下：

```
Switch# show running-config
Building configuration...
Current configuration: 318 bytes
!
version 1.0
!
hostname Switch
vlan 1
!
end
Switch#
```

第三步：进行具体任务配置。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip default-gateway 192.168.0.1 !设置交换机默认网关，实现跨网段管理交换机
Switch(config)# interface vlan 1
Switch(config if)# ip address 192.168.0.2 255.255.255.0
```

```
Switch(config)#exit
Switch(config)#enable secret level 1 5 star
Switch(config)#enable secret level 15 5 star
Switch(config)#radius-server host 192.168.0.185 auth-port 1812
!指定 RADIUS 服务器的地址及 UDP 认证端口
Switch(config)#aaa accounting server 192.168.0.185    !指定记账服务器的地址
Switch(config)#aaa accounting acc-port 1813           !指定记账服务器的 UDP 端口
Switch(config)#aaa authentication dot1x               !开启 AAA 功能中的 802.1x 认证功能
Switch(config)#aaa accounting                         !开启 AAA 功能中的记账功能
Switch(config)#radius-server key star                 !设置 RADIUS 服务器认证字
Switch(config)#snmp-server community public rw
          !为通过简单网络管理协议访问交换机设置认证名(public 为默认认证名)并分配读写权限
Switch(config)#interface fastEthernet 0/4        !实验中将在 4 号接口启动 802.1x 的认证
Switch(config-if)#dot1x port-control auto         !设置该接口参与 802.1x 认证
Switch(config-if)#exit
Switch(config)#exit
Switch#write
Building configuration...
[OK]
Switch#
```

验证测试：将两台 PC(使用 192.168.0.0/24 网段的地址，客户端 PC 使用地址 192.168.0.44/24，服务器使用地址 192.168.0.185/24)连接到交换机除 4 号端口外的其他任意两个端口上，在任何一个 PC 上进行连通性测试(ping)。在客户端上使用命令"ping 192.168.0.185"能够 ping 通。命令执行结果如图 4-68 所示。

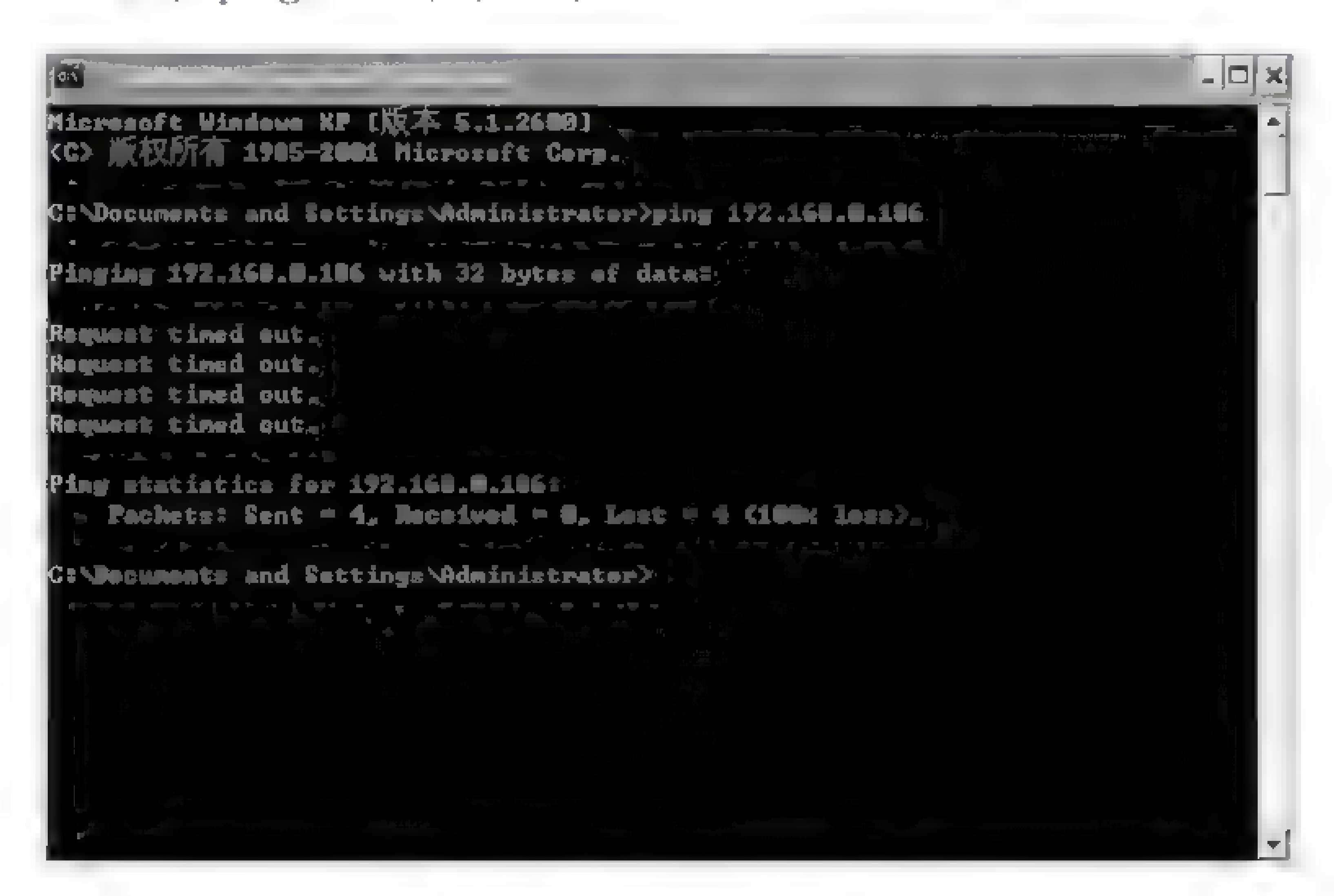


图 4-68　ping 测试结果(一)

将客户端 PC 或服务器 PC 接到 4 号端口，在其中的一台 PC 上 ping 另一台 PC，则不能够 ping 通。命令结果如图 4-69 所示。

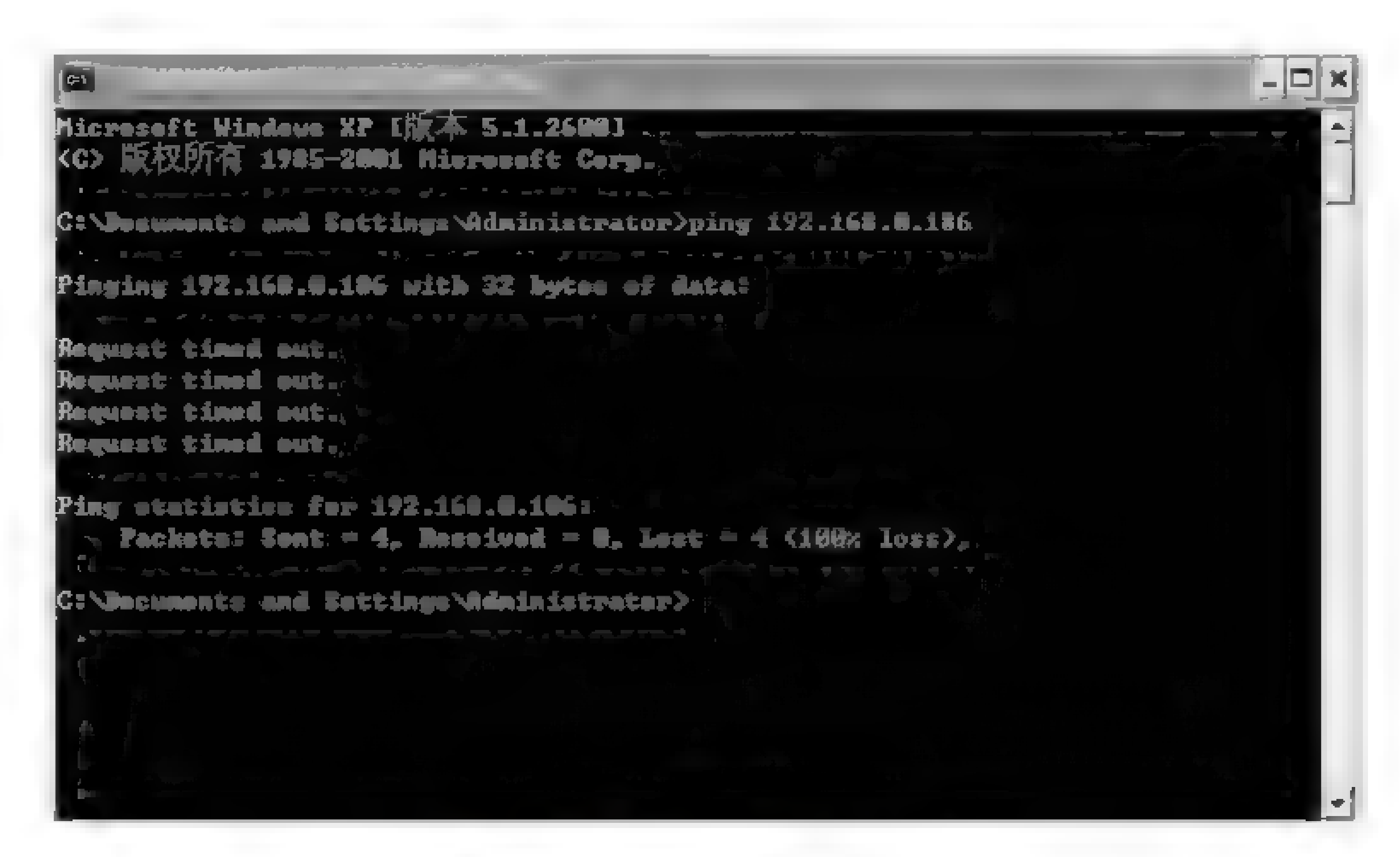


图 4-69　ping 测试结果(二)

思考训练(评估)

1. 思考与提高

(1) 什么是网络安全?

(2) 什么是 802.1 认证?

(3) 什么 ACL 访问控制列表?

(4) 什么是防火墙?

(5) 什么是 VPN?

2. 实训

(1) 构建相应的网络环境,配置 802.1 认证。

(2) 标准 ACL 配置与调试。设计标准 ACL,首先使得 PC1 所在的网络不能通过路由器 R1 访问 PC2 所在的网络,然后使得 PC2 所在的网络不能通过路由器 R2 访问 PC1 所在的网络。网络拓扑如图 4-70 所示。

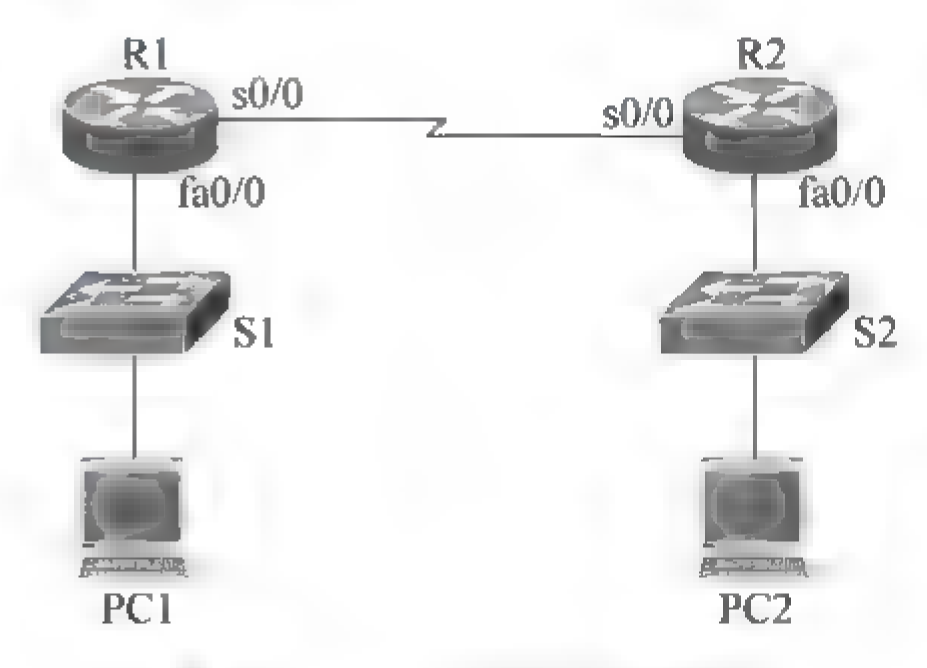


图 4 70　ACL 网络拓扑结构

(3) 构建相应的网络环境,配置 VPN 网络。

学习情境5　无线网络配置

任务情境(资讯)

随着市场的发展，无线网络占据了越来越大的份额，ThreeFour Software软件公司也在业务发展的过程中感受到无线网络的重要性。

小王是网管员，一天，公司的同事打来电话，要给客户共享一个资料，现场没有交换机，且同事与客户均没有移动存储设备，同事携带一条网线，但与客户的网卡均不支持网线自适应功能。小王了解到，同事与客户各有一块无线网卡，所以他指导同事用两块无线网卡进行联络，完成资料共享。

后来客户提出需求，要进行网络部署，但不巧的是，该客户的办公地点是一栋比较旧的建筑，不适合进行有线网络的部署。为了使客户能够正常通信并且实现资源共享，小王建议他使用RG-WG54P架设无线局域网。

由于业务拓展，在离公司总部不远的地方开设了一家门市，门市的员工要和总部通信。由于网络布线有困难，公司决定采用无线技术让门市的员工接入，接入时采用802.1x用户身份验证，并用WAPI和SSID加密，防止别的无线用户接入公司网络。

下面以锐捷公司的产品为例来完成任务。

任务分析(决策)

上述情境遇到3个核心问题，即构建自组网模式无线网络、构建基础结构模式无线网络和无线网络隐秘技术。下面先讨论基础理论。

1. 无线网络

所谓无线网络，就是利用无线电波作为信息传输的媒介构成的无线局域网(WLAN)。它与有线网络的用途十分类似，最大的不同在于传输媒介不同，用无线电技术取代网线，可以和有线网络互为备份。

目前主流应用的无线网络分为GPRS手机无线网络上网和无线局域网两种方式。应该说，GPRS手机上网方式是目前真正意义上的无线网络，它是一种借助移动电话网络接入Internet的无线上网方式，只要用户所在城市开通了GPRS业务，用户在任何一个角落都可以通过笔记本电脑上网。不过，由于目前GPRS上网资费高，速率较慢(最快仅相当于56Kbps Modem)，所以用户群很小。本节不将这种无线上网方式作为重点，仅围绕无线局域网方式来展开讨论。

首先说，无线网络并不是神秘之物，它是相对于目前普遍使用的有线网络而言的一种全新的网络组建方式。很多人称无线网络是一种“甩开辫子”的全新上网方式，在一定程度上扔掉了有线网络必须依赖的网线。这样一来，用户可以坐在家里的任何一个角落，抱着笔记本电脑，享受网络的乐趣，而不像从前那样必须要迁就于网络接口的布线位置，家里也不会被一根根的网线弄得乱七八糟。

无线上网需要哪些设备呢？既然没有了网线而改用信号方式进行连接，起信号接收作用的无线网卡显然是一个必不可少的部件。目前，网卡主要有 MINI PCI、PC 卡和 USB 三种规格，前两种规格在笔记本电脑中应用比较广泛。其中，MINI PCI 为内置型无线网卡，迅驰机型和非迅驰的无线网卡标配机型均使用这种无线网卡。其优点是无须占用 PC 卡插槽，并且免去了随时身携一张 PC 卡的麻烦，更重要的是由于此类机型的信号天线大都放置在 LCD 的两侧，相对位置较高，可以获得更好的信号接收质量，信号好于自身集成天线的 PC 卡无线网卡。

如果笔记本电脑没有标配无线网卡，并且预留了 MINI-PCI 插槽和信号天线，用户可以购买一块本机 BIOS 支持的 MINI-PCI 型的无线网卡安装于机器中，经过简单的天线连接就可以使用了；否则，只能考虑采用 PC 卡无线网卡。

有了信号的接收设备，自然还要有无线信号的发射源，才能组成一个完整的网络环境。如果用户居住和工作的环境提供无线网络信号，那么有一张无线网卡就已足够；否则，用户还需要购置一个设备，那就是无线接入点（AP，Access Point）。AP 的作用是给无线网卡提供网络信号。目前市售的 AP 主要分不带路由功能的普通 AP 和带路由功能的 AP 两种。简单地说，前者是最基本的 AP，仅仅提供无线信号发射的功能；而路由 AP 可以为拨号接入 Internet 的 ADSL 等提供自动拨号功能，也就是说，当客户机开机时，网络就自动接通了，不再需要手动拨号。另外，路由 AP 具备更完善的安全防护功能。

2. 常见无线网络标准简介

① IEEE 802.11a：IEEE 无线网络标准，指定最大 54Mbps 数据传输速率和 5GHz 工作频段。

② IEEE 802.11b：IEEE 无线网络标准，指定最大 11Mbps 数据传输速率，使用 2.4GHz 频段。

③ IEEE 802.11g：IEEE 无线网络标准，指定最大 54Mbps 和 108Mbps 数据传输速率，使用 2.4GHz 频段，可向下兼容 802.11b。

④ IEEE 802.11n 草案：IEEEE 无线网络标准，指定最大 300Mbps 数据传输速率，使用 2.4GHz 频段。目前，该标准为草案，但产品层出不穷。

目前，IEEE 802.11b 最常用，但 IEEE 802.11g 更具下一代标准的实力，802.11n 也在快速发展中。

3. AP 接入点

AP 接入点（Access Point，又称无线局域网收发器）是用于无线网络的无线 HUB，是无线网络的核心。它是移动计算机用户进入有线以太网骨干的接入点，AP 可以简便地

安装在天花板或墙壁上。根据接入网络所采用的无线标准不同，它在开放空间的最大覆盖范围可达300m，无线传输速率可达11～300Mbps。

AP接入点是无线接入的最前端设备，它一般通过一根或几根天线来完成信息的传递，无线局域网天线可以扩展无线网络的覆盖范围，把不同的办公大楼连接起来。这样，用户可以随身携带笔记本电脑在大楼之间或在房间之间移动。

由于无线接入不像有线接入那样是可见的，对于AP接入点来讲，要限定有效范围空间，造成接入点与接入点之间产生交接问题。在无线网络标准中，主要通过以下几个方面来解决：

① 动态速率转换：当射频情况变差时，可将数据传输速率从11Mbps降低为5.5Mbps，2Mbps或1Mbps。

② 漫游支持：当用户在楼房或公司部门之间移动时，允许在访问点之间进行无缝连接。IEEE 802.11无线网络标准允许用户在不同的无线网桥网段中使用相同的信道，或在不同的信道之间漫游。

③ 负载均衡：当AP变得负载过大或信号减弱时，NIC能更改与之连接的访问点AP，自动转换到最佳可用的AP，以提高性能。

④ 扩谱技术：是一种在20世纪40年代发展起来的调制技术，它在无线电频率的宽频带上发送传输信号，包括跳频扩谱(FHSS)和直接顺序扩谱(DSSS)两种。跳频扩谱被限制在2Mbps数据传输率，并建议用在特定的应用中。对于其他所有的无线局域网服务，直接顺序扩谱是更好的选择。在IEEE 802.11b标准中，允许采用DSSS的以太网速率达到11Mbps。

⑤ 自动速率选择功能：IEEE 802.11无线网络标准允许移动用户设置在自动速率选择(ARS)模式下。ARS功能会根据信号的质量及与网桥接入点的距离自动为每条传输路径选择最佳的传输速率。该功能还可以根据用户的不同应用环境设置成不同的固定应用速率。

⑥ 电源消耗管理功能：IEEE 802.11还定义了MAC层的信令方式，通过电源管理软件的控制，使移动用户的电池能具有最长寿命。电源管理软件会在无数据传输时使网络处于休眠(低电源或断电)状态，这样可能丢失数据包。为此，IEEE 802.11规定了AP应具有缓冲区存储信息，处于休眠的移动用户会定期醒来恢复该信息。

4. SSID

SSID是Service Set Identifier的缩写，意思是服务集标识。SSID技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都需要独立的身份验证，只有通过身份验证的用户才可以进入相应的子网络，防止未被授权的用户进入本网络。

SSID也可以写为ESSID，用来区分不同的网络，最多可以有32个字符。无线网卡设置了不同的SSID，就可以进入不同网络。SSID通常由AP广播出来，通过操作系统自带的扫描功能可以查看当前区域内的SSID。出于安全考虑，可以不广播SSID，此时用户要手工设置SSID才能进入相应的网络。简单地说，SSID是一个局域网的名称，只有设置相同SSID的电脑才能互相通信。

通俗地说，SSID 是用户给自己的无线网络所取的名字。需要注意的是，同一生产商推出的无线路由器或 AP 使用了相同的 SSID，一旦那些企图非法连接的攻击者利用通用的初始化字符串来连接无线网络，就极易建立起一条非法的连接，给用户的无线网络带来威胁。因此，建议将 SSID 命名为有个性的名字。

无线路由器一般都会提供"允许 SSID 广播"功能。如果用户不想让自己的无线网络被别人通过 SSID 名称搜索到，那么最好"禁止 SSID 广播"。这时，无线网络仍然可以使用，只是不会出现在其他人所搜索到的可用网络列表中。通过禁止 SSID 广播设置后，无线网络的效率会受到影响，但以此换取安全性的提高，还是值得的。由于没有进行 SSID 广播，该无线网络被无线网卡忽略了，尤其是在使用 Windows XP 管理无线网络时，达到了"掩人耳目"的目的。

任务设计（计划）

在简单了解用于无线网络连接的基本方法后，根据公司的具体情况提出以下 3 个任务来解决实际问题：

任务 5.1　构建自组网模式无线网络

任务 5.2　构建基础结构模式无线网络

任务 5.3　无线网络的安全、加密部署

任务实施（实施）

任务 5.1　构建自组网模式无线网络

情境回顾：小 E 接到公司同事电话，在现场，同事与客户之间仅有无线网卡可以实现通信。在这种情况下，根据前述对无线网络组网模式的了解，小 E 决定指导同事用两块无线网卡组成自组网模式无线网络，实现与客户的资源共享。

任务所需设备为 WG54U（802.11g 无线局域网外置 USB 网卡，2 块），网络拓扑如图 5-1 所示。

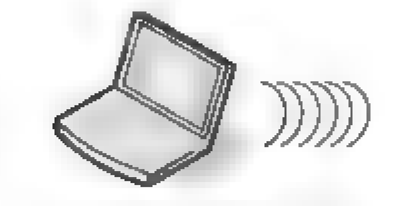
1. 安装 WG54U

① 把 WG54U 适配器插入到计算机空闲的 USB 端口，系统会自动搜索到新硬件并且提示安装设备的驱动程序。

② 选择"从列表或指定位置安装"并插入驱动光盘或软盘，选择驱动所在的相应位置（软驱或者指定的位置），然后单击"下一步"按钮。

③ 计算机将会找到设备的驱动程序，按照屏幕指示安装 54Mbps 无线 USB 适配器，然后单击"下一步"按钮。

④ 单击"完成"按钮结束安装，屏幕的右下角出现无线网络已连接的图标，如图 5-2 所示，包括速率和信号强度。





PC1: 192.168.1.1/24　　PC2: 192.168.1.2/24

图 5-1　简单无线网络构建



图 5-2　无线网卡任务栏图标

2. 设置无线网卡

设置无线网卡之间相连的 SSID 为"ruijie"，具体操作步骤如图 5-3～图 5-5 所示。



图 5-3　无线网络连接

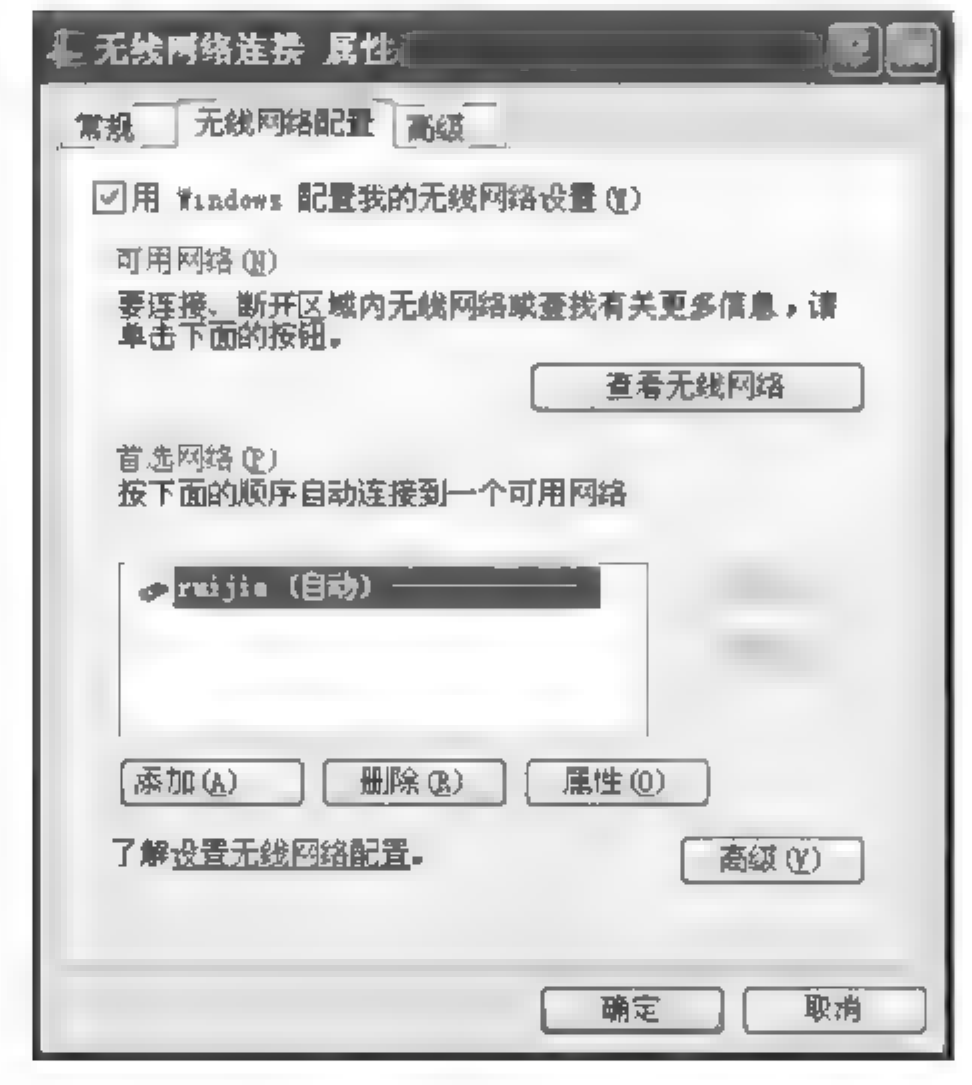


图 5-4　配置网卡

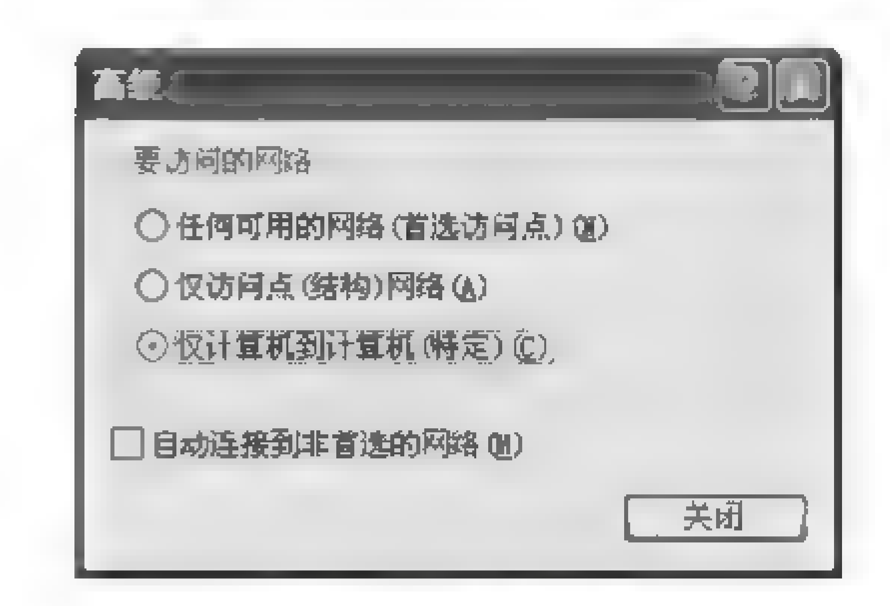


图 5-5　高级设置

在无线网络配置一栏中，单击"添加"按钮，添加一个新的 SSID 为"ruijie"。在"高级"一栏中选择"仅计算机到计算机"模式，或者通过 RG-WG54U 产品中的无线网络配置软件，选择自组网模式(Ad Hoc)模式。

3. 设置 PC2 无线网卡的 IP 地址

将 PC2 的 IP 地址设置为 192.168.1.2(见图 5-6)。PC1 的配置方法与 PC2 相同,但 PC1 的 IP 地址要设置为 192.168.1.1,否则与 PC2 的地址会有冲突。

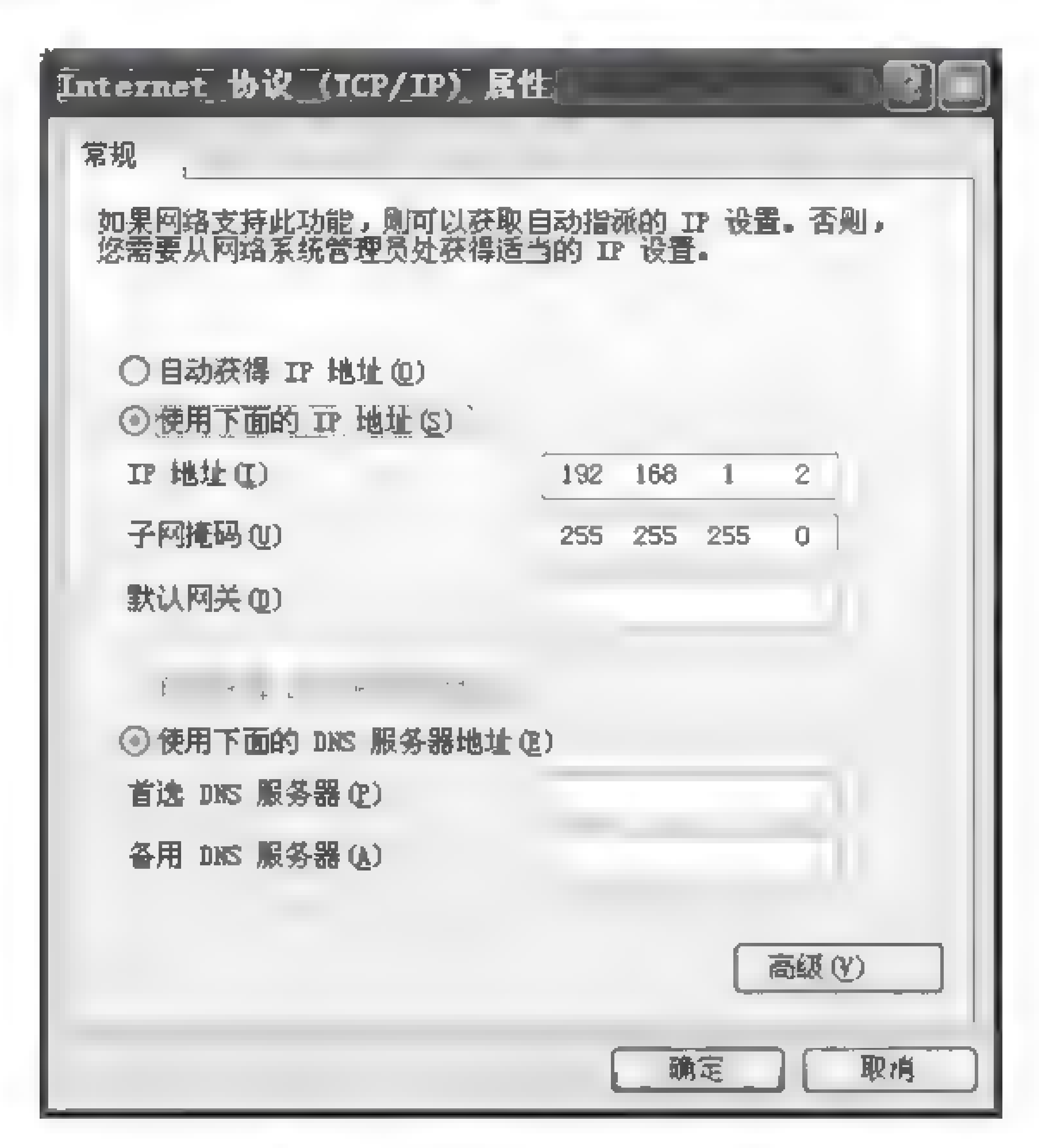


图 5-6　配置 PC2 的 IP 地址

4. 测试 PC2 与 PC1 的连通性

在 PC2 上用 Ping 命令:Ping 192.168.1.1(PC1 的 IP 地址),测试连通性,测试成功,如图 5-7 所示。

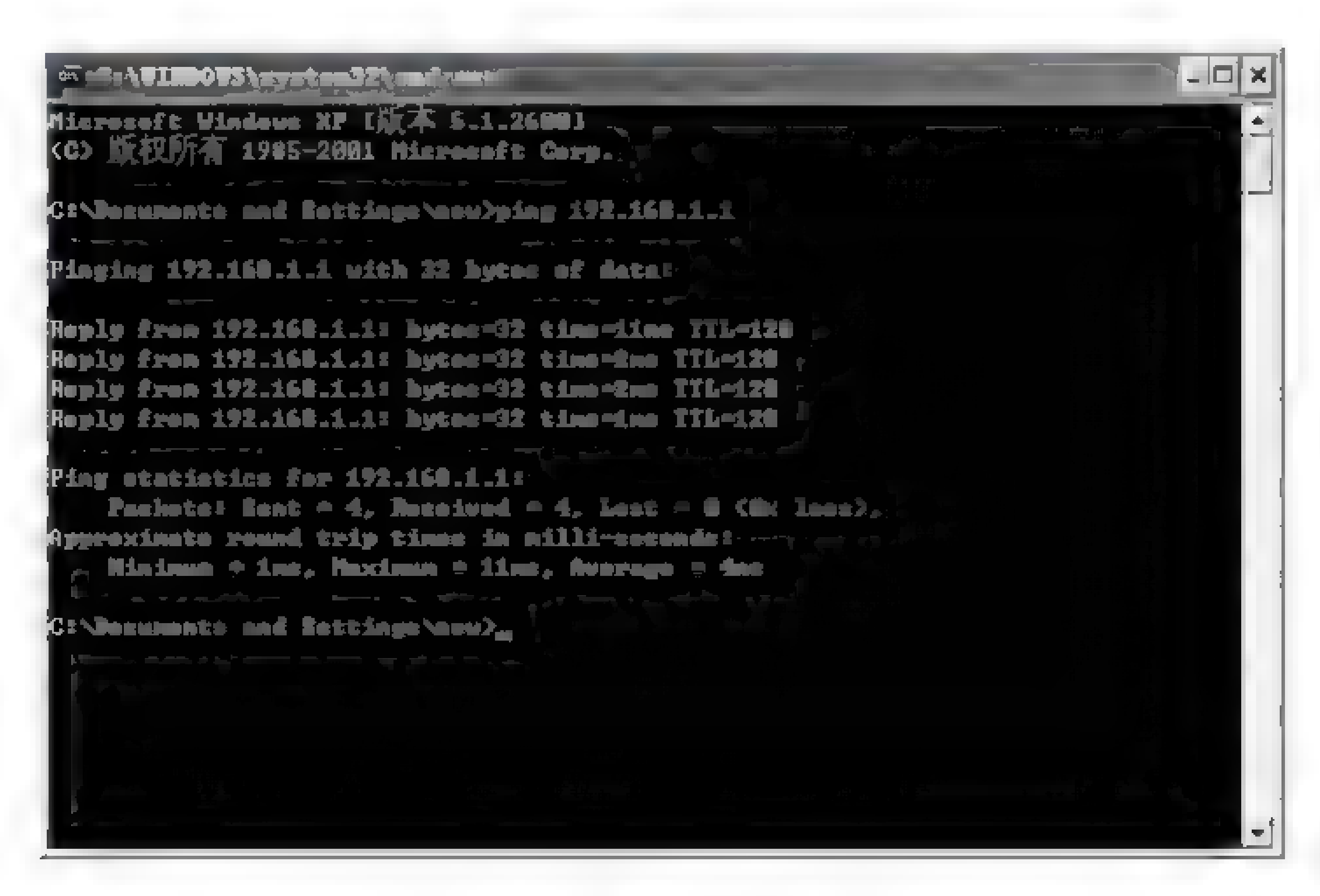


图 5-7　测试连通性

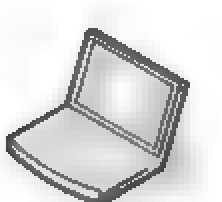
任务 5.2 构建基础结构模式无线网络

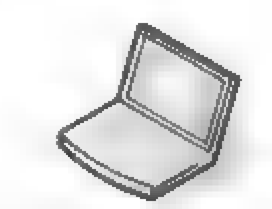
情境回顾：根据客户提出的网络部署要求，由于办公环境不适合采用有线网络，为了使得局域网用户能够正常通信并且实现资源共享，建议架设基础结构模式无线网络。

任务所需设备：RG-WG54U（802.11g 无线 LAN 外置 USB 网卡，2 块）和 RG-WG54P（无线局域网接入设备，1 台）。网络拓扑如图 5-8 所示。

RG-WG54P: AP-TEST
ESSID: ruijie
RG-WG54P 管理地址：192.168.1.1/24







PC1 无线 IP 地址：1.1.1.2/24　　PC2 无线 IP 地址：1.1.1.36/24
PC1 以太网 IP 地址：192.168.1.23/24

图 5-8　构建简单无线网络

1. 安装无线网卡 RG-WG54U

① 把 RG-WG54U 适配器插入到计算机空闲的 USB 端口，系统会自动搜索到新硬件并且提示安装设备的驱动程序。

② 选择"从列表或指定位置安装"并插入驱动光盘或软盘，选择驱动所在的相应位置（软驱或者指定的位置），然后单击"下一步"按钮。

③ 计算机将找到设备的驱动程序，按照屏幕指示安装 54Mbps 无线 USB 适配器，然后单击"下一步"按钮。

④ 单击"完成"按钮结束安装，屏幕的右下角出现无线网络已连接的图标，包括速率和信号强度，如图 5-9 所示。



图 5-9　无线网卡任务栏图标

2. 配置无线 AP(RG-WG54P)

第一步，将所需的设备连接起来，如图 5-10 所示。

注：这是实物连接图，由于 RG WG54P 有一个供电的适配器是支持以太网供电的，故需要正确地按图示连接。

第二步，配置各种设备，如图 5-11 所示。

因为 RG-WG54P 出厂时管理地址默认为 192.168.1.1/24，需要将 PC1 的网卡 IP 地址为 192.168.1.23/24。





图 5-10　实物连接图

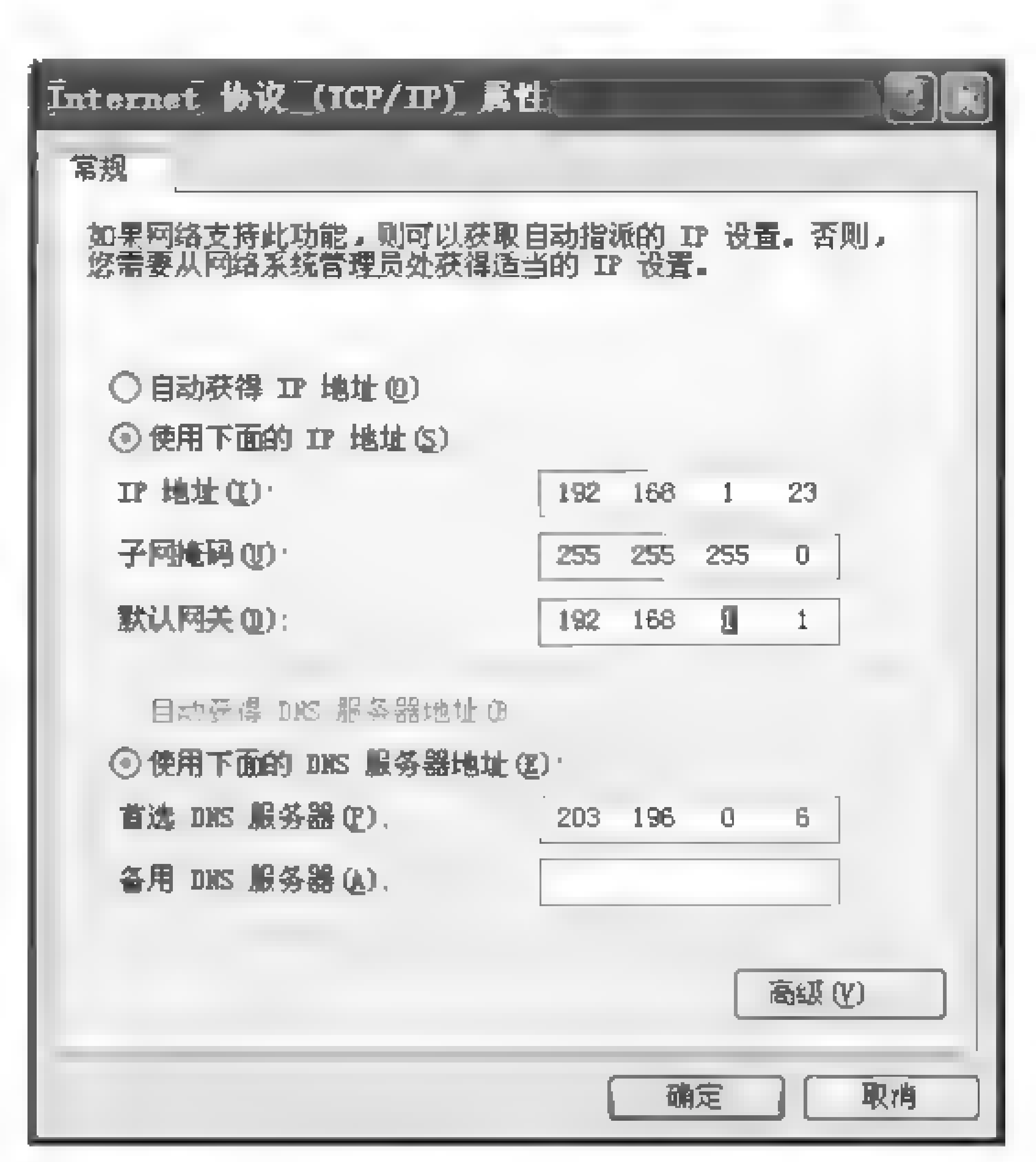


图 5-11　IP 配置

在 IE 浏览器中输入 http://192.168.1.1，登录到 RG-WG54P 的管理界面，输入默认密码“default”，如图 5-12 所示。



图 5-12　无线 AP 登录界面

RG WG54P 登录界面的常规信息如图 5 13 所示。



图 5-13　基本配置

在常规设置中修改接入点名称为 AP-TEST(此名称为任意设置),设置无线模式为 AP,ESSID 为 ruijie(ESSID 名称可任意设置)、信道/频段为 01/2412MHz,模式为混合模式(此模式可根据无线网卡类型具体设置)。

第三步,生效配置。配置完成后,单击"确定"按钮,使 RG-WG54P 应用新的设置,如图 5-14 所示。



图 5 14　完成配置

3. 配置 SSID

为 PC1 与 PC2 安装 RG WG54U 配置软件，设置 SSID 为 ruijie，选择组网模式为基础结构模式(Infrastructure)，如图 5-15 所示。

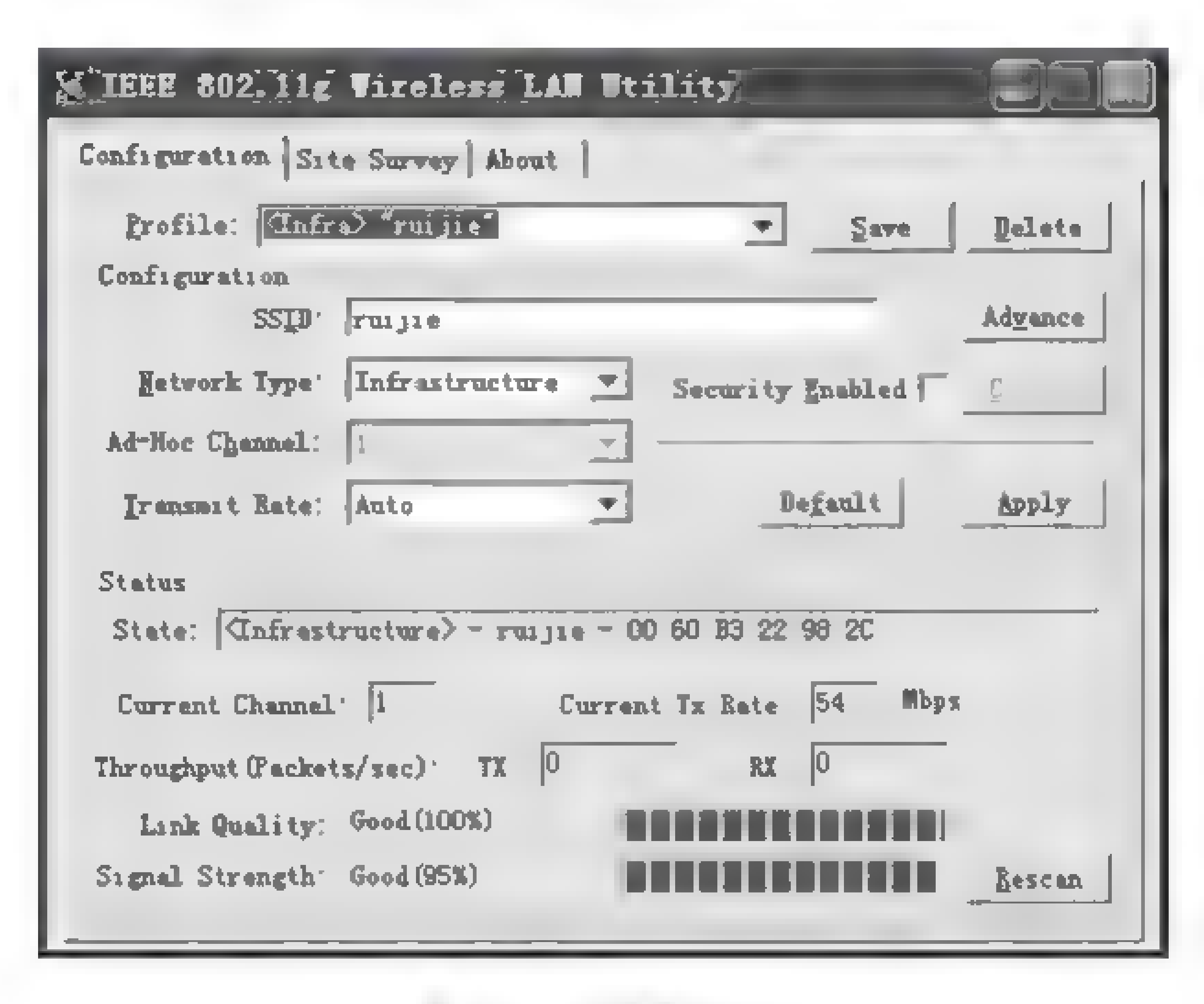


图 5-15　配置 SSID

4. 加入 ESSID

将 PC1 与 PC2 的 RG-WG54P 网卡加入到 ruijie 这个 ESSID，如图 5-16 所示。

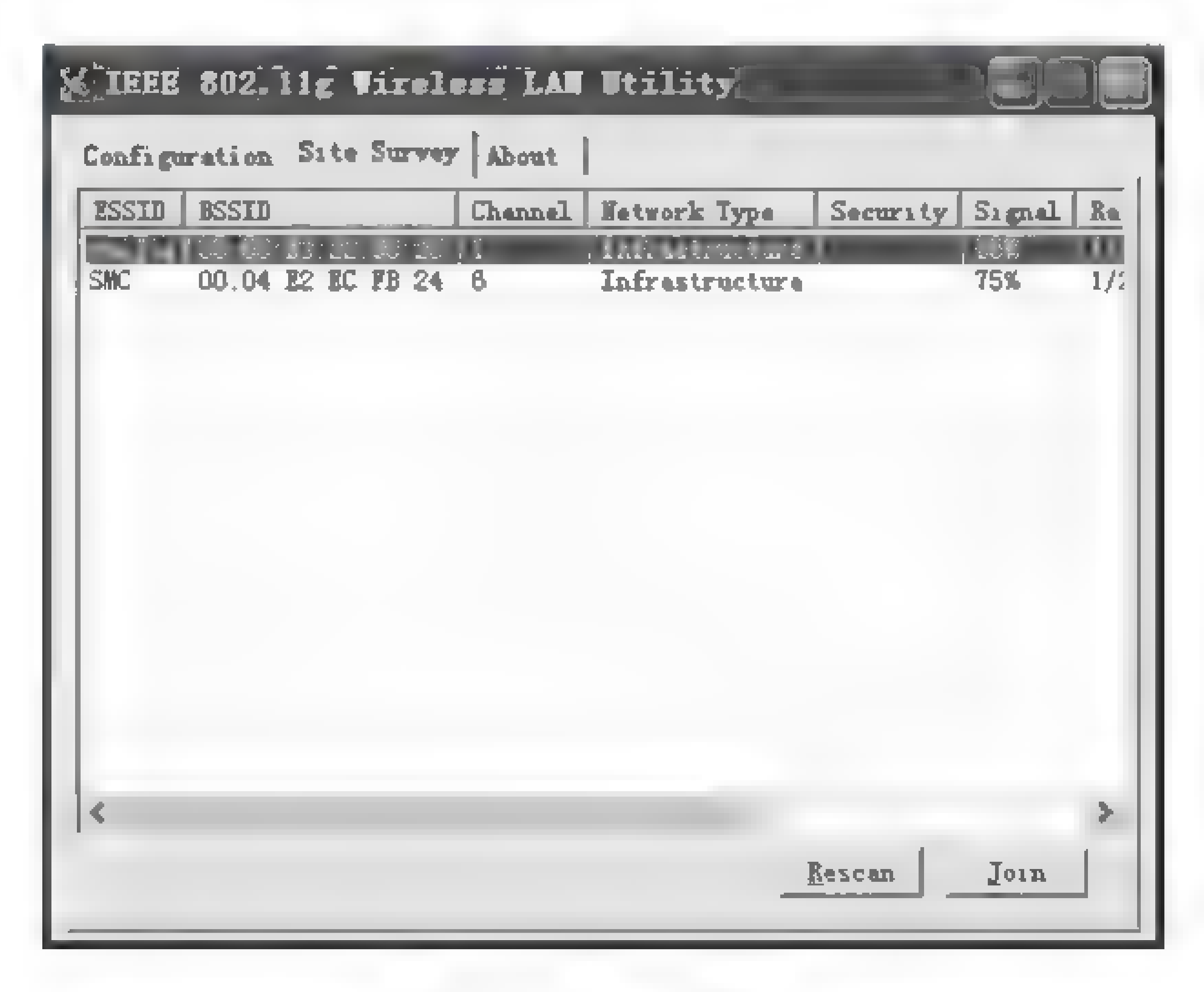


图 5-16　加入 ESSID

选中“ruijie”，然后单击右下角的“Join”按钮。

5. 配置 IP 地址

配置 PC1 地址为 1.1.1.2，PC1 地址为 1.1.1.36，保证在同一网段即可(图 5-17 中为 PC2 地址配置，PC1 与 PC2 地址配置方法相同)。

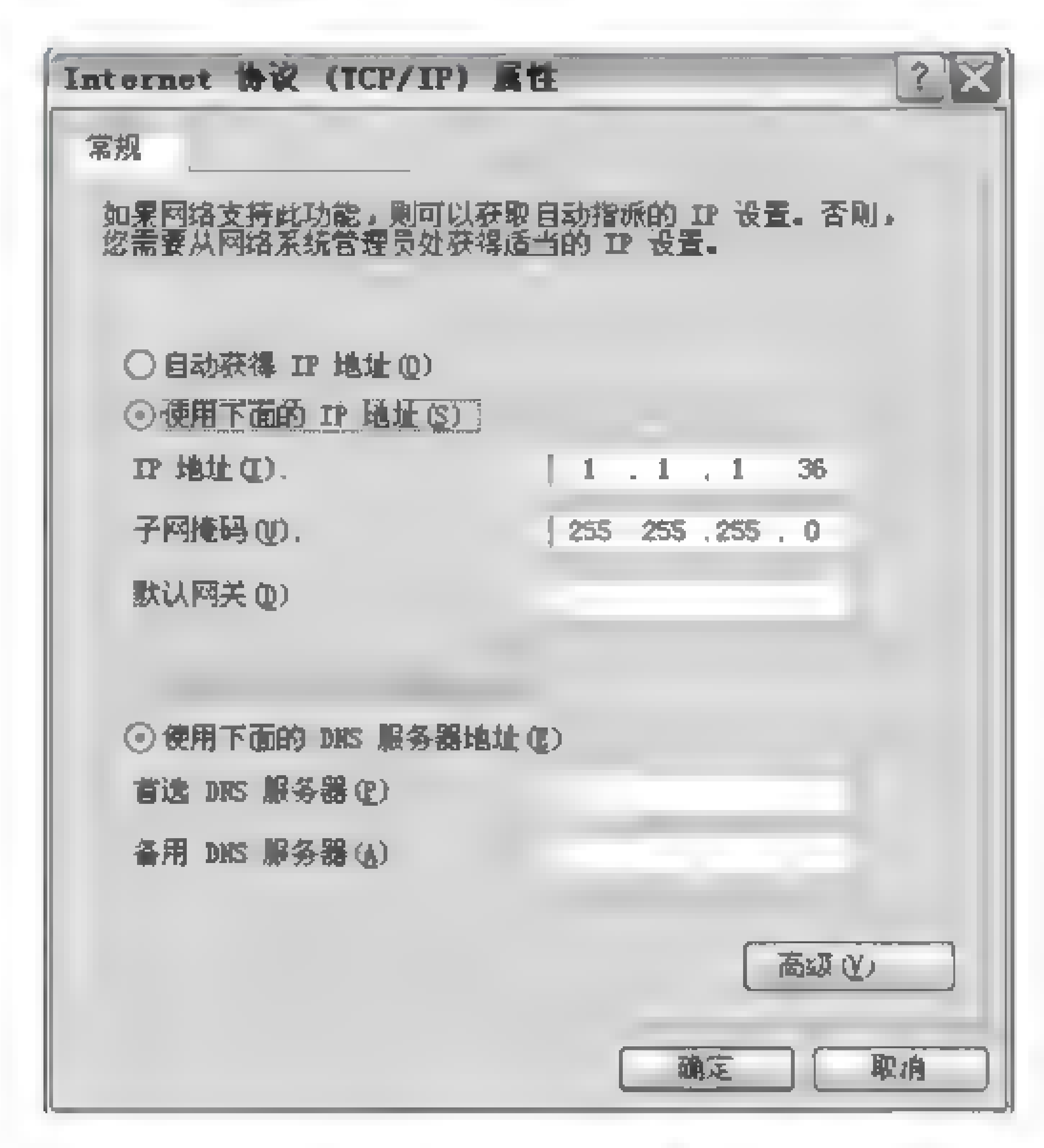


图 5-17　IP 设置

6. 测试连通性

测试 PC1 与 PC2 的连通性，如图 5-18 所示。

```
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\new>ping 1.1.1.36

Pinging 1.1.1.36 with 32 bytes of data:

Reply from 1.1.1.36: bytes=32 time=11ms TTL=128
Reply from 1.1.1.36: bytes=32 time=2ms TTL=128
Reply from 1.1.1.36: bytes=32 time=2ms TTL=128
Reply from 1.1.1.36: bytes=32 time=2ms TTL=128

Ping statistics for 1.1.1.36:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\Documents and Settings\new>_
```

图 5 18　测试连通性

任务 5.3　无线网络的安全、加密部署

情境回顾：作为公司的网络管理人员，按公司业务发展要求，在公司门市部署无线网络；同时为了保证网络的安全与保密，要求在接入的时候采取 802.1x 用户身份验证，并用 WAPI 和 SSID 加密，防止别的无线用户接入公司的网络。

任务所需设备：RG-108M 无线网卡两块，RG-108M 无线 AP 一台。网络拓扑如图 5-19 所示。

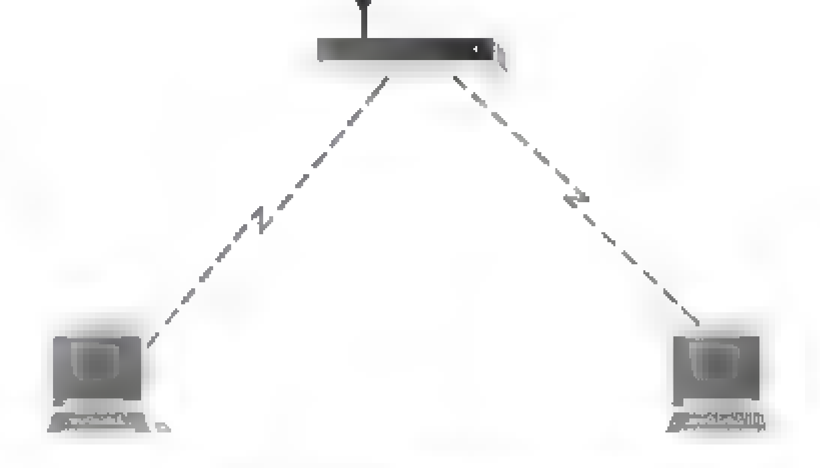


图 5-19　典型无线网络

1. 配置无线 AP

进入无线 AP 的界面，然后根据具体要求来配置，操作步骤如图 5-20～图 5-22 所示。

为了保证无线网络的安全，需要在 AP 配置中将 WEP(Wired Equivalent Privacy，有线等效协议)选择为“enable”，以实现对无线传递数据的加密。



图 5-20　配置无线 AP

2. 设置在 AP 端 802.1x 验证

认证类型选择 802.1x 加密方式，长度选择 64bits，其他默认，如图 5-23 所示。

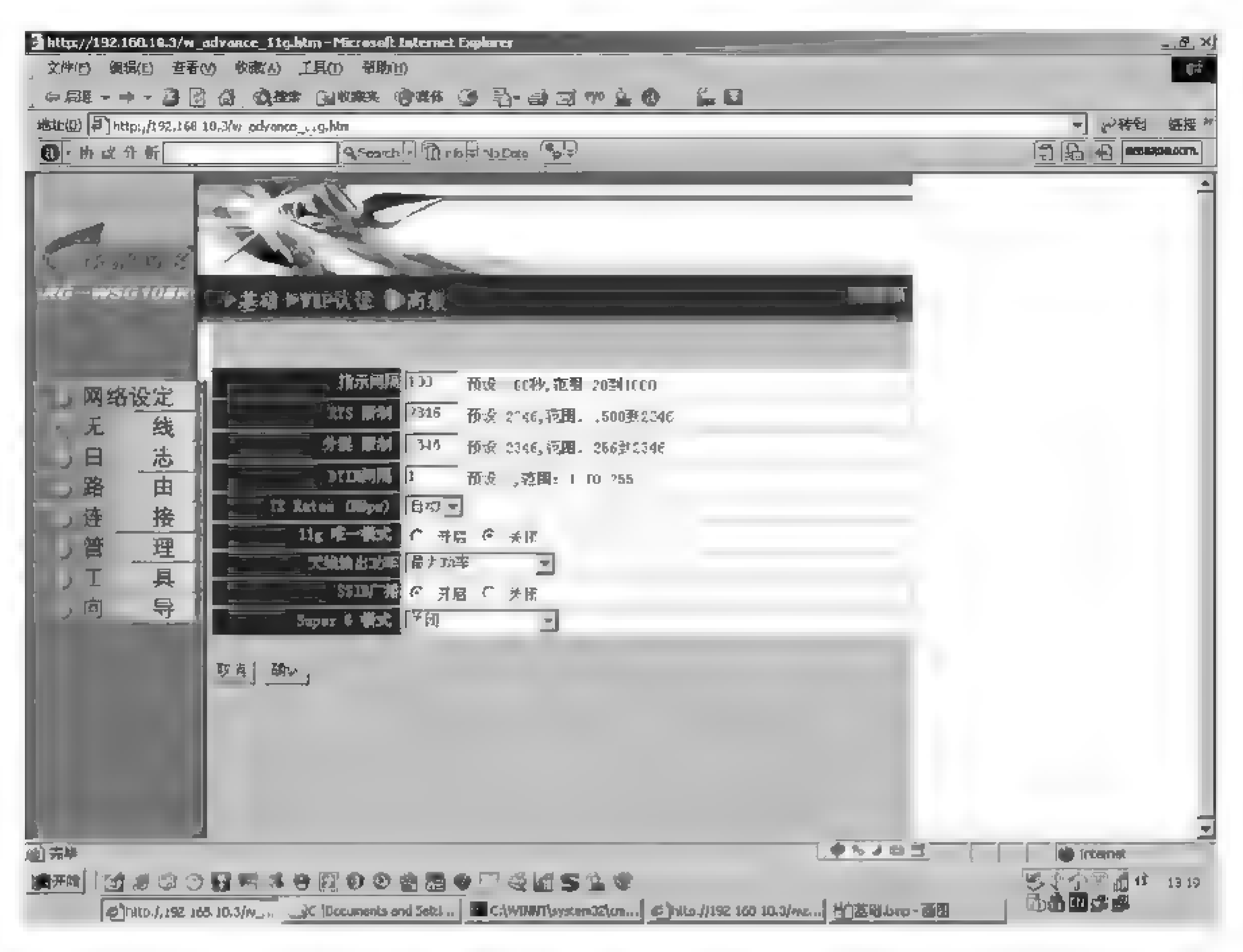


图 5-21　配置无线 AP 参数

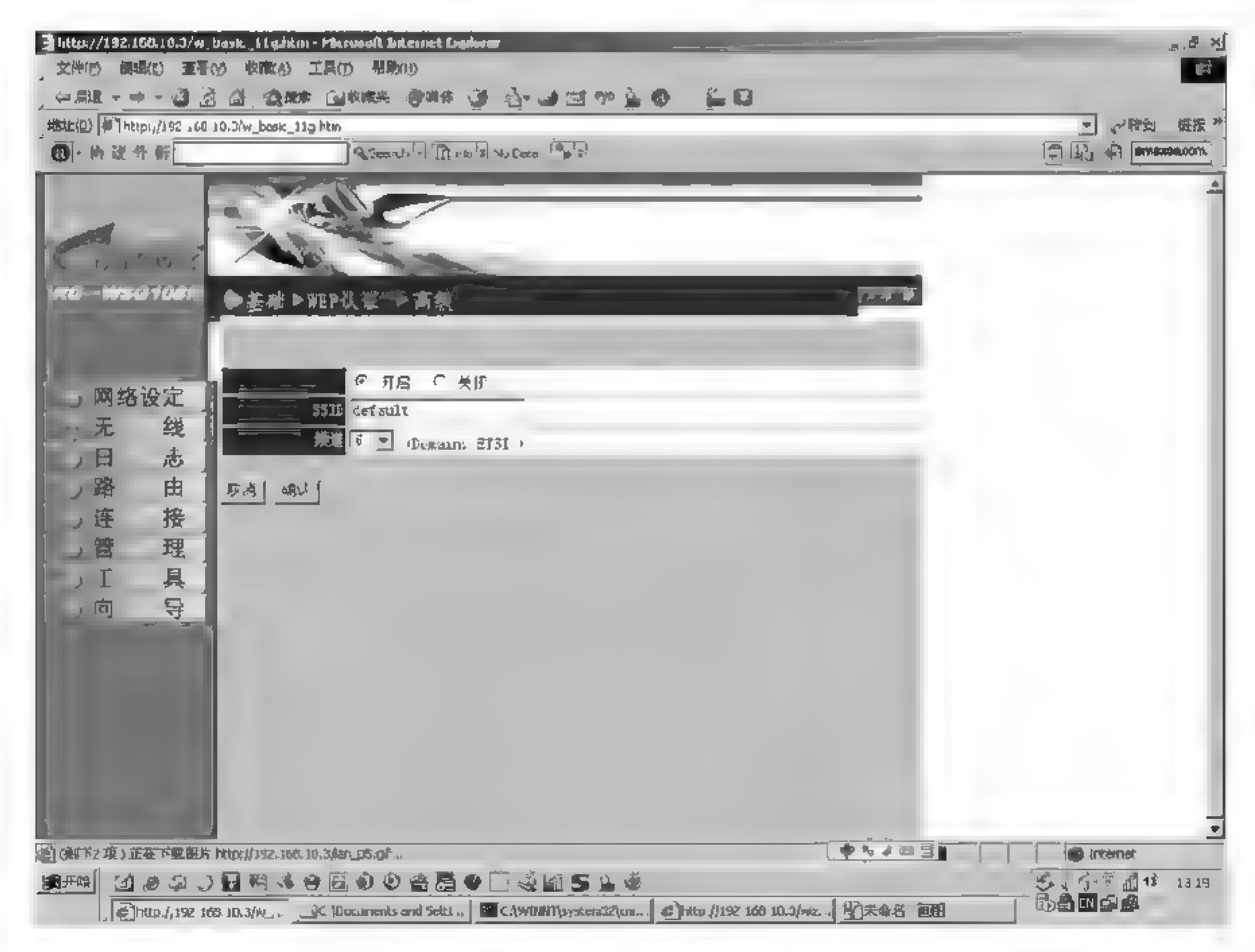


图 5 22　完成配置

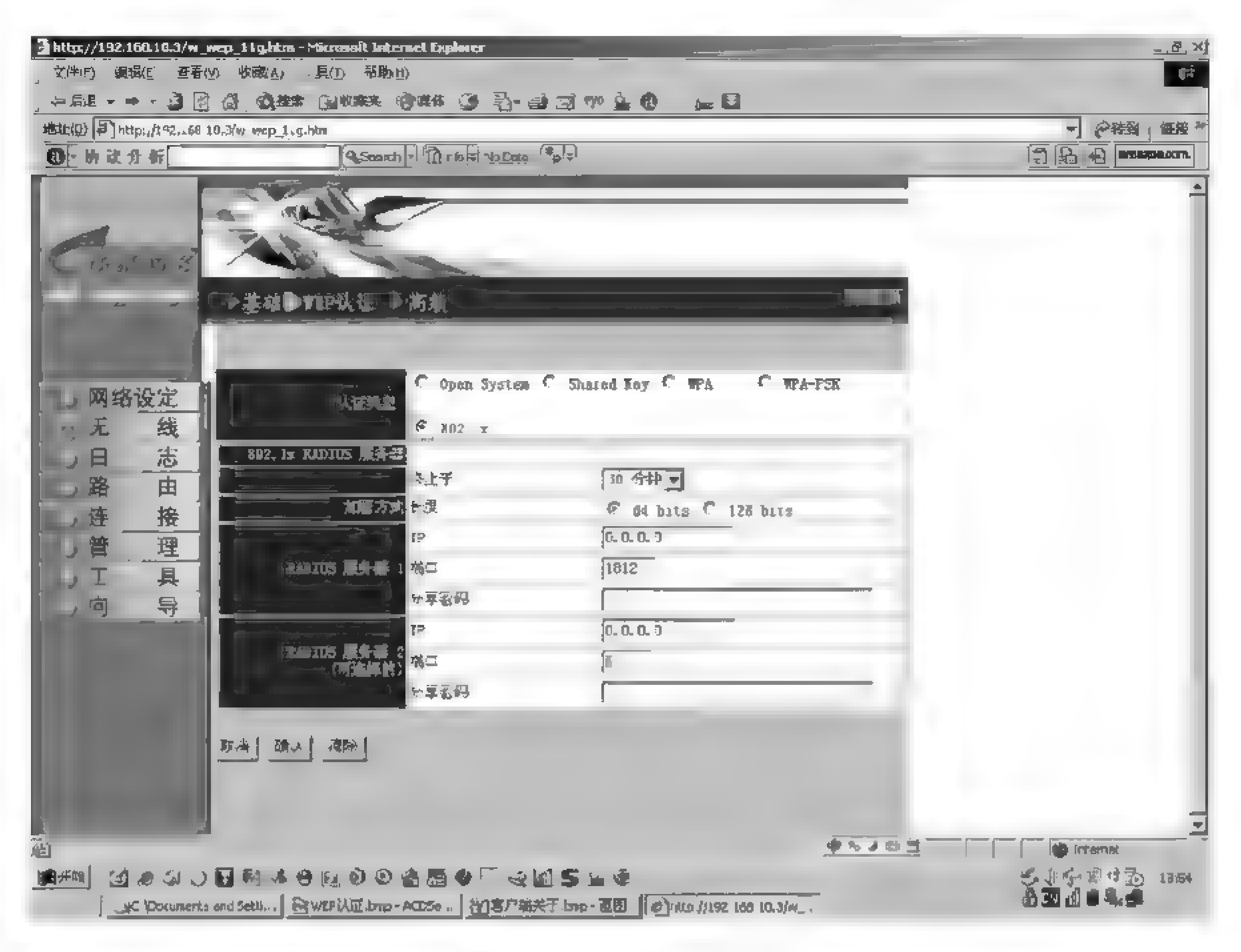


图 5-23 802.1x 验证

3. 配置客户端

在"基础设置"项中,SSID 选择 default,无线模式选择普通接收模式,其他配置为默认,如图 5-24 所示。

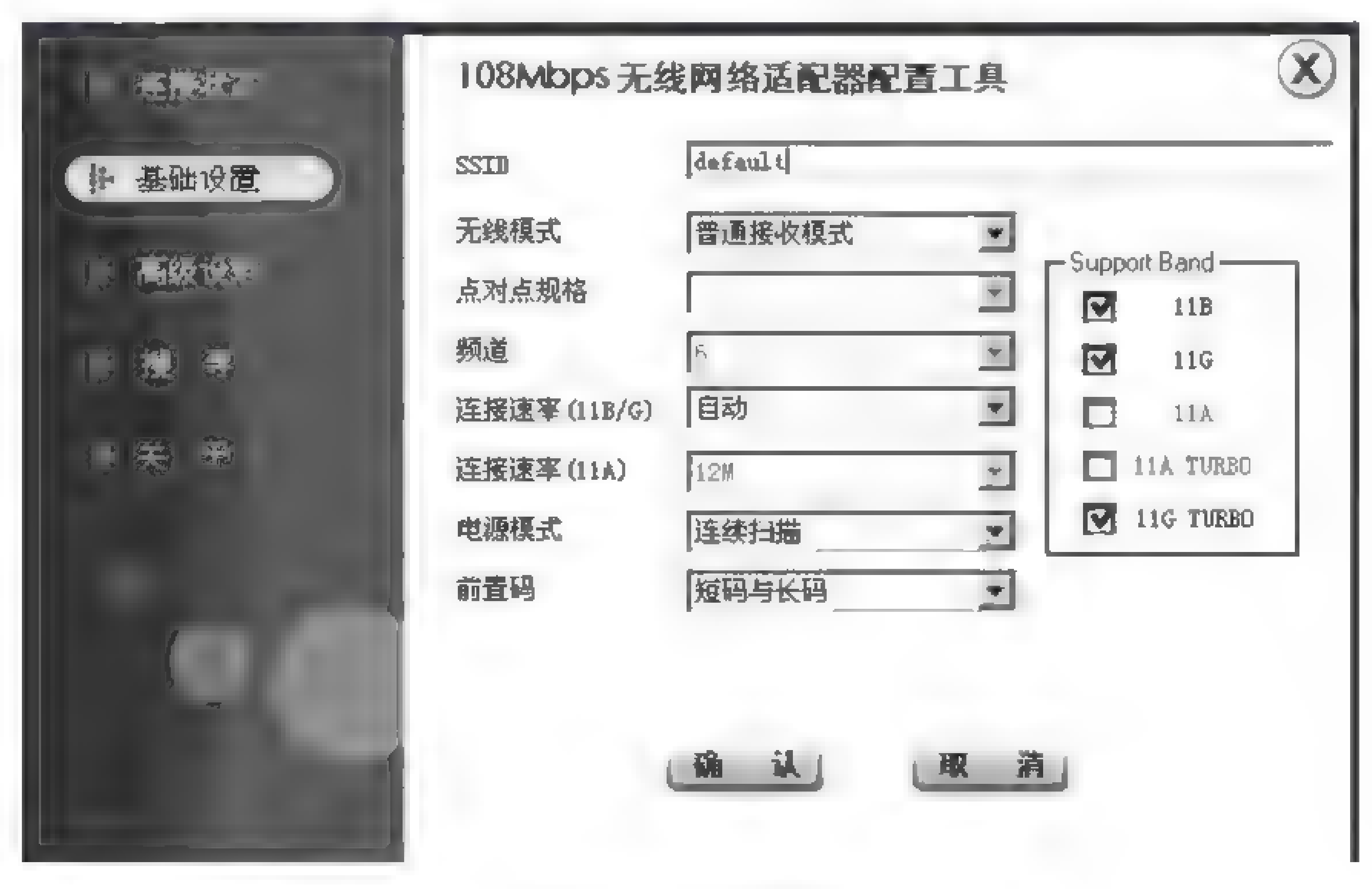


图 5 24 客户端配置

4. 配置客户端接入认证

客户端接入认证在“高级设定”项中设置，加密技术选“开启”，验证模式选择“认证”，其他默认，如图 5-25 所示。

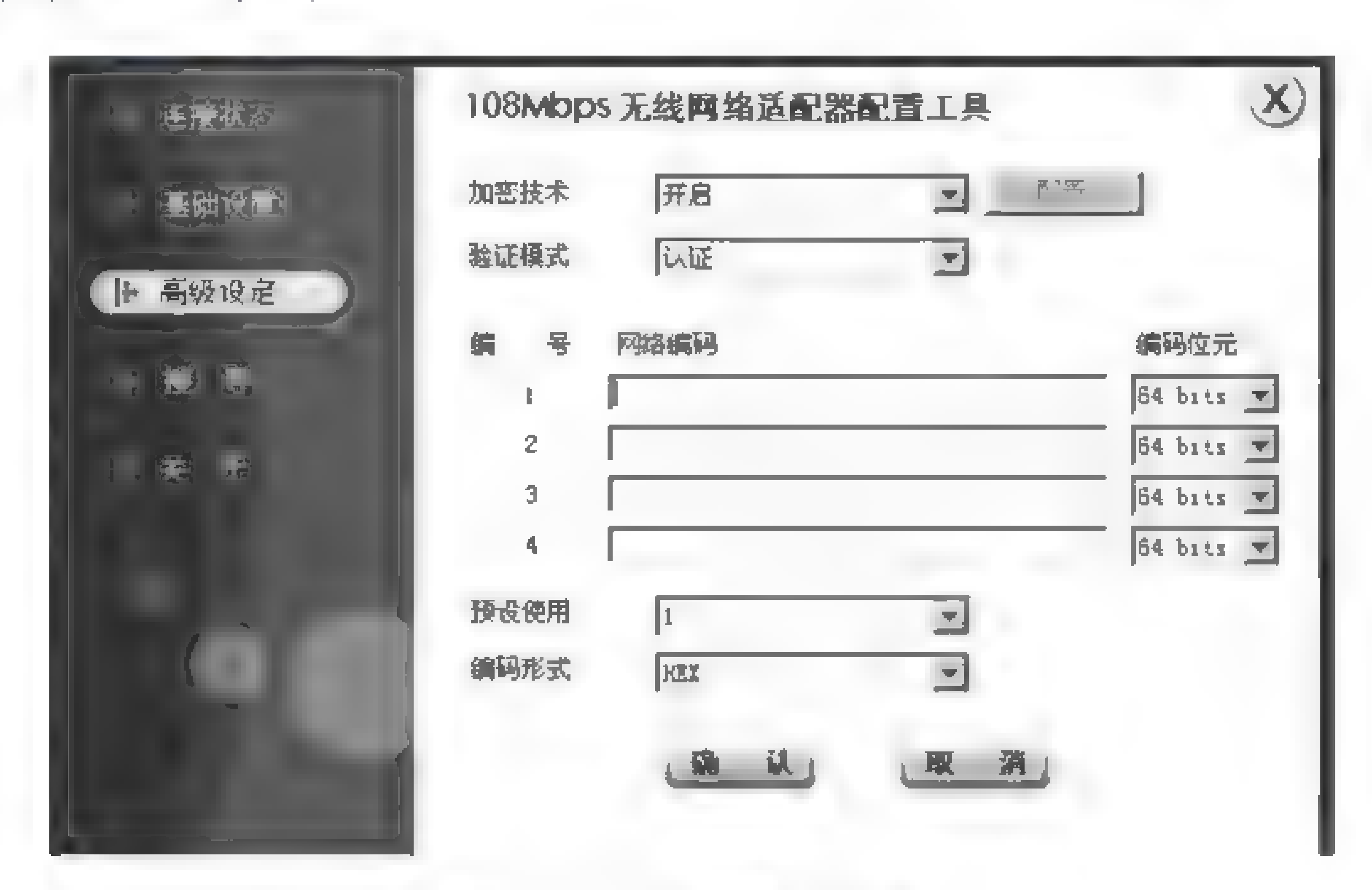


图 5-25 客户端接入认证

规律总结(检查)

① 两台移动设备的无线网卡的 SSID 必须一致，才能实现通信。

② 无线网卡默认的信道为 1，如遇其他系列网卡，要根据实际情况调整无线网卡的信道，使多块无线网卡的信道一致。

③ 两块无线网卡的 IP 地址设置为同一网段，才能组成一个能够互相通信的网络。

④ 无线网卡通过自组网式无线网络互联，对两块网卡的距离有限制，工作环境下一般不建议超过 10m。

⑤ 无线网卡通过基础结构模式互联，覆盖距离可以达到 100～300m。

⑥ 无线网络隐秘技术目前解决的是对在无线网络中传递的数据进行加密，但由于其自身密钥长度等的缺陷，对其入侵的难度相对较小，因此这种无线网络隐秘技术仅用于阻止初级入侵用户的入侵。

思考训练(评估)

1. 思考与提高

(1) 什么是无线网络？

(2) 常见无线网络标准有几种？

(3) 什么是 AP(接入点)？

(4) 什么是 SSID？

2. 实训

(1) 某办公室有三名工作人员，均有笔记本电脑(配无线网卡)。请你根据所学知识为他们搭建一个网络，实现相互之间的资源共享。要求写出实施方案与具体配置过程。

(2) 同第(1)题场景，办公室仅有一个网络信息接入点，现要求采用无线方式实现每个人均能接入 Internet。请根据所学知识提出构建方案与具体配置过程。

学习情境 6　网络综合配置应用

任务情境(资讯)

随着公司业务的不断开展，ThreeFour Software 公司借助几年来在 IT 市场上积累的经验，成立了网络集成项目部。项目部成立后，承接了两项网络综合项目，通过项目的实施，使得部门成员得到了很好的锻炼。现将两个项目的具体情况描述如下。

1. 企业双出口网络集成

某中型企业要求按照"安全性、可管理性、稳定性"的原则，对原有网络进行更新改造，具体要求如下：

① 为了保证网络出口的稳定性和可靠性，企业向 ISP 申请了两条 Internet 线路，用作负载均衡和冗余备份。

② 为了保证网络的安全性、可靠性，企业要求核心设备支持防 DDoS(Distribution Denial of Service，分布式拒绝服务攻击)攻击、防恶意的 IP 扫描。病毒侵入与非法攻击是企业网络很大的安全隐患，不发作则已，一发作就是大问题。因此，要求内部网络能实现在核心层、接入层防止网络蠕虫病毒扩散，要求核心和接入网络设备能支持 VLAN 的划分，降低网络内广播数据包的传播，提高带宽资源利用率。

③ 网络设备需支持灵活多样的管理方式，以减轻管理、维护的难度。

2. 大型单核心项目集成

某大型企业随着现代化管理进程的推进，需要在现有网络的基础上进行升级改造，将目前已有各分支机构网络连到一起，实现内部专业业务核算网络与外部访问数据的共享与互通，同时要保证内部各业务子网的独立与安全。这个项目集合了交换路由基础、OSPF、802.1q、VLAN、NAT、SNMP、ACL 访问控制、安全控制等众多网络综合业务，对参与网络集成的人员提出了很高的要求。

下面以锐捷公司的产品为例来介绍。

任务分析(决策)

上述情境遇到的核心问题是构建网络所需的设备以及如何根据网络实际情况来配置设备。为此，需要注意以下几点：

1. 做好需求分析

需求分析是要了解局域网用户现在想要实现什么功能、未来三年需要什么功能、后续

投入有多大，为网络设计提供必要的参考。

2. 确定网络类型和工作模式

(1) 确定网络类型

现在的局域网市场几乎完全被性能优良、价格低廉、升级和维护方便的以太网所占领，所以一般的局域网都选择以太网连接，并且以星型连接。

(2) 确定网络带宽和网络设备

一个网络(数百台至上千台计算机构成的局域网)可以在逻辑上分为以下几个层次：核心层、分布层和接入层。在中小规模网络(几十台至几百台计算机构成的局域网)中，可以将核心层与分布层合并，称为折叠主干，简称主干，称接入层为分支。对于由几十台计算机构成的小型网络，可以不必采取分层设计的方法。在工作模式上，根据需要，采用集中模式或分散计算模式，或者两种结合的共用网络模式。所以，先要了解每个使用端的应用要求，以确定客户端设备。

目前快速以太网能够满足网络数据流量不是很大的中小型局域网的需要。但是在计算机数量超过数百台，或网络数据流量比较大的情况下，应采用千兆以太网技术，以满足对网络主干数据流量的要求。

网络主干和分支方案确定之后，就可以选定交换机和路由产品了。现在市场上的交换机品牌不下几十种。性能最高的当属 Cisco，3Com，Avaya 等国外交换机品牌，这些产品占领了高端市场，价格非常昂贵；以锐捷、神州数码、D-Link、TP-LINK 为代表的国内交换机厂商的产品具有非常高的性能价格比，也可以选择。交换机的数量由网络拓扑结构来决定。

任务设计(计划)

为了体现现代网络构建的具体情况，本节提出以下两个典型的任务来解决在网络建设中可能遇到的问题：

任务 6.1　中小企业双出口网络

任务 6.2　大型(单核心)网络综合项目

任务实施(实施)

任务 6.1　中小企业双出口网络

情境回顾：根据前述任务情境描述，该企业网络改造首先要解决的关键点是双出口的负载均衡与冗余备份；然后是根据企业要求在设备上进行网络安全的配置与管理，以满足企业提出的“安全性、可管理性、稳定性”原则。

下面根据企业提出的改造原则和具体工作需求分别进行需求分析，以确定网络改造升级所需的设备及设备配置与管理资料。

1. 需求分析

需求 1：为了保证网络出口的稳定性、可靠性，企业向 ISP 申请了两条 Internet 线路用作负载均衡和冗余备份。

分析 1：出口的两台设备连接两条线路，可采用 VRRP 技术实现负载均衡，使得客户端连接外网透明化。

需求 2：为了保证网络的安全性、可靠性，企业要求核心设备支持防 DDoS 攻击、防恶意的 IP 扫描。因此，要求内部网络能实现在核心层、接入层防止网络蠕虫病毒扩散，要求核心和接入网络设备能支持 VLAN 的划分，降低网络内广播数据包的传播，提高带宽资源利用率，防止广播风暴的产生。

分析 2：以上是对产品本身功能的需求，核心可采用 RG-S6800E 系列交换机，接入采用安全接入交换机 RG-S2100 系列。

需求 3：网络具有可管理性，网络设备支持灵活多样的管理方式。

分析 3：所有网络设备均配置远程管理功能，使得用户可以在本地登录各个设备。

2. 网络拓扑结构的提出

网络拓扑结构(如图 6-1 所示)。

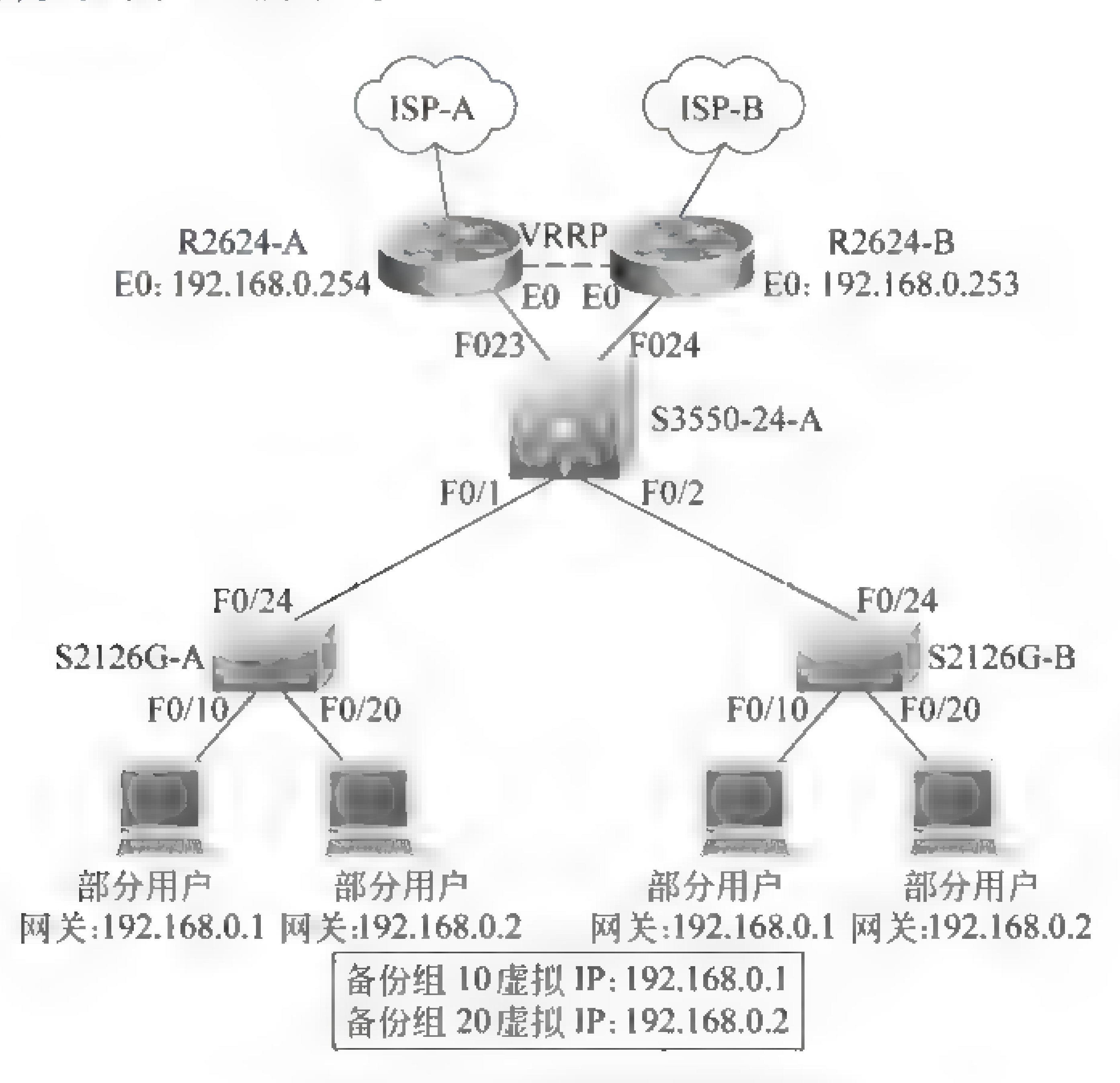


图 6-1 双出口网络拓扑结构图

3. 地址规划

地址规划如表 6-1 所示。

表 6-1　IP 地址规划

设　　备	IP　地　址	备　　注
R2624 A	192.168.0.254/24	R2624 A E0
R2624 B	192.168.0.253/24	R2624 B E0
虚拟备份组 10	192.168.0.1/24	虚拟备份组 10
虚拟备份组 20	192.168.0.2/24	虚拟备份组 20

4. 实施步骤

具体配置包括以下几个部分：

① 网络设备基本配置及基本测试；

② VRRP 功能配置及验证；

③ VRRP 功能测试。

第一步：设备基本配置及网络测试。

(1) S2126G-A 交换机基本配置(用作二层设备)

```
hostname S2126G-A
vlan 1
end
```

(2) S2126G-B 交换机基本配置(用作二层设备)

```
hostname S2126G-B
vlan 1
end
```

(3) S3550-24-A 交换机基本配置(用作二层设备)

```
hostname S3550-24-A
vlan 1
end
```

(4) R2624-A 路由器基本配置

```
conf t
hostname R2624-A
enable password star
interface FastEthernet0
ip address 192.168.0.254 255.255.255.0
no shut
exit
line vty 0 4
password star
login
```

(5) R2624 B 路由器基本配置

```
conf t
hostname R2624-B
!
enable password star
!
interface FastEthernet0
ip address 192.168.0.253 255.255.255.0
no shut
exit
line vty 0 4
password star
login
```

(6) 测试网络连通性

通过 ping 测试,网络通信正常。

① 在 R2624-A 上,使用 ping 命令来测试到 R2624-B 的连通性。

```
R2624-A# ping 192.168.0.253
Type escape sequence to abort.
Sending 5,100-byte ICMP Echoes to 192.168.0.253, timeout is 2 seconds: .!!!!
Success rate is 80 percent (4/5),round-trip min/avg/max=1/1/4ms
```

② 在 R2624-A 上,使用 ping 命令来测试到 R2624-A 的连通性。

```
R2624-B# ping 192.168.0.254
Type escape sequence to abort.
Sending 5,100-byte ICMP Echoes to 192.168.0.254, timeout is 2 seconds: !!!!!
Success rate is 100 percent (5/5),round-trip min/avg/max=1/1/4 ms
```

第二步:在路由器上配置 VRRP 功能。

VRRP 功能是通过配置两台 R2624 路由器实现的。根据项目方案,采用两个备份组,虚拟出两个 IP 地址:虚拟备份组 10、IP 地址为 192.168.0.1/24;虚拟备份组 20,IP 地址为 192.168.0.2/24。

(1) R2624-A 基本配置

```
interface FastEthernet0
vrrp 10 priority 105            !设置虚拟组优先级为 105,默认为 100
vrrp 10 ip 192.168.0.1          !配置虚拟组地址
vrrp 20 ip 192.168.0.2          !配置虚拟组地址
exit
```

(2) R2624-B 基本配置

```
interface FastEthernet0
vrrp 10 ip 192.168.0.1
vrrp 20 priority 150
vrrp 20 ip 192.168.0.2
exit
```

(3) VRRP 验证

通过(1)和(2)的基本配置，虚拟组 10 以在 R2624 A 为主路由器，R2624 B 为备份路由器；虚拟组 20 以 R2624 A 为备份路由器，R2624 B 为主路由器。使用如下命令验证 VRRP 配置：

```
R2624-A# show vrrp brief                           !显示当前 vrrp 状态
Interface          Grp Pri Time   Own Pre State   Master addr   Group addr
FastEthernet0      10   105  ——     P  Master   192.168.0.254  192.168.0.1
FastEthernet0      20   100  ——     P  Backup   192.168.0.253  192.168.0.2
R2624-B# show vrrp brief                           !显示当前 vrrp 状态
Interface          Grp Pri Time   Own Pre State   Master addr   Group addr
FastEthernet0      10   100  ——     P  Backup   192.168.0.254  192.168.0.1
FastEthernet0      20   150  ——     P  Master   192.168.0.253  192.168.0.2
```

使用如下命令查看详细的 VRRP 信息：

① 在 R2624-A 上查看 vrrp 信息

```
R2624-A# show vrrp                        !显示当前 vrrp 状态
FastEthernet0-Group 10                    !以太网接口名称及接口上设置的 vrrp 备份组号
State is Master                                   !vrrp 备份组状态
Virtual IP address is 192.168.0.1 configured      !备份组 10 虚拟 ip 地址
Virtual MAC address is 0000.5e00.010A             !备份组 10 虚拟 mac 地址
Advertisement interval is 1 sec                   !vrrp 通告时间间隔
Preemption is enabled                             !设置了抢占模式
min delay is 0 sec
Priority is 105                                   !优先级
Master Router is 192.168.0.254 (local), priority is 105
                                    !虚拟组 10 master 路由器 ip 地址及 master 路由器优先级
Master Advertisement interval is 1 sec    !master 路由器通告时间间隔
Master Down interval is 3 sec             !master 路由器失效判断时间间隔
FastEthernet0-Group 20                    !以太网接口名称及接口上设置的 vrrp 备份组号
State is Backup                           !vrrp 备份组状态
Virtual IP address is 192.168.0.2 configured       !备份组 20 虚拟 ip 地址
Virtual MAC address is 0000.5e00.0114              !备份组 20 虚拟 MAC 地址
Advertisement interval is 1 sec                    !vrrp 通告时间间隔
Preemption is enabled
Min delay is 0 sec
Priority is 100                                    !设置优先级
Master Router is 192.168.0.253,pritority is 150   !虚拟组 20 master 路由器 ip 地址及 master 路
由器优先级
Master Advertisement interval is 1 sec             !master 路由器通告时间间隔
Master Down interval is 3 sec                      !master 路由器失效判断时间间隔
```

② 在 R2624 B 上查看 vrrp 信息

```
R2624-B# show vrrp
    State is Backup FastEthernet0-Group 10

    Virtual IP address is 192.168.0.1 configured
```

```
Virtual MAC address is 0000.5e00.010A
Advertisement interval is 1 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.0.254,pritority is 105
Master Advertisement interval is 1 sec
Master Down interval is 3 sec
FastEthernet0-Group 20
State is Master
Virtual IP address is 192.168.0.2 configured
Virtual MAC address is 0000.5e00.0114
Advertisement interval is 1 sec
Preemption is enabled
min delay is 0 sec
Priority is 150
Master Router is 192.168.0.253 (local), priority is 150
Master Advertisement interval is 1 sec
Master Down interval is 3 sec
```

(4) 网络连通性测试

对于接在接入层设备 S2126G 上的用户，为其分配 IP 地址为 192.168.0.3/24～192.168.0.252/24，网关可以指向 192.168.0.1 或者 192.168.0.2。由于在出口路由器上配置了 VRRP，可以为网络提供冗余备份和负载均衡功能。

```
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix.:
        IP Address........................ : 192.168.0.234
        Subnet Mask....................... : 255.255.255.0
        Default Gateway................... : 192.168.0.1          !终端用户以虚拟组 10 为网关
D:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
                                          !经测试 pc 192.168.0.234 到网关 192.168.0.1 通信正常
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix.:
        IP Address...................... : 192.168.0.234
        Subnet Mask..................... : 255.255.255.0
        Default Gateway................. : 192.168.0.2 !终端用户以虚拟组 20 为网关
D:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<10ms TTL=255
                                          !经测试 pc 192.168.0.234 到网关 192.168.0.2 通信正常
```

第三步：VRRP 功能测试。测试 VRRP 冗余备份与负载均衡功能。

根据 VRRP 功能，在主路由器失效的情况下，备份路由器会在一定的时间里切换为主路由器；在使用了抢占模式后，若路由器故障恢复后，VRRP 会重新计算，主路由器切换到备份状态，故障路由器为主状态。

（1）网络正常运行情况下，VRRP 状态及网络连通性

```
R2624-A# show vrrp brief                    !显示 R2624-A vrrp 状态
Interface          Grp Pri Time  Own Pre State   Master addr   Group addr
FastEthernet0      10  105  ——    P  Master   192.168.0.254  192.168.0.1
FastEthernet0      20  100  ——    P  Backup   192.168.0.253  192.168.0.2
R2624-B# show vrrp brief                                      !显示 R2624-B vrrp 状态
Interface          Grp Pri Time  Own Pre State   Master addr   Group addr
FastEthernet0      10  100  ——    P  Backup   192.168.0.254  192.168.0.1
FastEthernet0      20  150  ——    P  Master   192.168.0.253  192.168.0.2
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
         Connection-specific DNS Suffix.:
         IP Address.......................  : 192.168.0.234
         Subnet Mask.....................   : 255.255.255.0
         Default Gateway...............     : 192.168.0.1
         !以虚拟组 10 为默认网关的终端用户
D:\>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
!经测试终端用户 pc 192.168.0.234 到网关 192.168.0.1 通信正常
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
         Connection-specific DNS Suffix.:
         IP Address.......................  : 192.168.0.234
         Subnet Mask.....................   : 255.255.255.0
         Default Gateway...............     : 192.168.0.2
D:\>ping 192.168.0.2
Pinging 192.168.0.2 with 32 bytes of data:
Reply from 192.168.0.2: bytes=32 time<10ms TTL=255
!经测试终端用户 pc 192.168.0.234 到网关 192.168.0.2 通信正常
```

（2）若 2624-A 路由器出现故障，VRRP 状态及网络的连通性

终端用户使用 ping 命令加"-t"参数来观察当路由器出现故障后网络连通性的变化，通过将 S3550-24-A 与 R2624-A 之间的线缆人为断开来模拟 R2624-A 路由器故障。

① 在网络正常运行时，网络通信正常。

```
D:\> ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
         Connection-specific DNS Suffix.:
         IP Address.......................  : 192.168.0.234
         Subnet Mask.....................   : 255.255.255.0
```

```
        Default Gateway...............  : 192.168.0.1
D:\>ping 192.168.0.1-t
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
......
!......表示 Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
!在网络正常运行时网络通信正常
```

② 当 R2624-A 出现故障时,网络连通性变化。

```
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix.:
        IP Address......................  : 192.168.0.234
        Subnet Mask.....................  : 255.255.255.0
        Default Gateway...............  : 192.168.0.1
D:\>ping 192.168.0.1-t
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Request timed out.
Request timed out.
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
......
!R2624-A 路由器出现故障后,网络出现中断,之后很快网络恢复网络连通性
```

③ 当 R2624-A 出现故障时,VRRP 状态变化情况。

```
R2624-B# show vrrp brief
Interface        Grp Pri Time  Own Pre State   Master addr    Group addr
FastEthernet0    10  100  ——     P   Master   192.168.0.253  192.168.0.1
FastEthernet0    20  150  ——     P   Master   192.168.0.253  192.168.0.2
```

④ R2624-A 出现故障到恢复正常的过程中,网络连通性变化。

```
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix.:
        IP Address......................  : 192.168.0.234
        Subnet Mask.....................  : 255.255.255.0
        Default Gateway...............  : 192.168.0.1
D:\>ping 192.168.0.1-t
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
!R2624-A 出现故障
Request timed out.
Request timed out.
```

```
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
……
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
!R2624-A 恢复正常时刻
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
Reply from 192.168.0.1: bytes=32 time<10ms TTL=255
……
!从 R2624-A 出现故障到恢复正常的过程中，网络在出现暂时中断之后恢复正常。在路由器
R2624-A 恢复正常后，网络切换回来，通信正常，不会发生中断
```

⑤ 从 2624-A 出现故障到恢复正常，VRRP 状态变化。

```
R2624-B# show vrrp brief
Interface         Grp Pri Time  Own Pre State  Master addr   Group addr
FastEthernet0     10  100  ——    P  Master  192.168.0.253  192.168.0.1
FastEthernet0     20  150  ——    P  Master  192.168.0.253  192.168.0.2
!R2624-A 发生故障，R2624-B 路由器 VRRP 状态，备份组状态发生变化。
R2624-B# show vrrp brief
Interface         Grp Pri Time  Own Pre State  Master addr   Group addr
FastEthernet0     10  100  ——    P  Backup  192.168.0.254  192.168.0.1
FastEthernet0     20  150  ——    P  Master  192.168.0.253  192.168.0.2
!当 R2624-A 恢复正常，R2624-B 路由器 VRRP 状态
R2624-A# show vrrp brief
Interface         Grp Pri Time  Own Pre State  Master addr   Group addr
FastEthernet0     10  105  ——    P  Master  192.168.0.254  192.168.0.1
FastEthernet0     20  100  ——    P  Backup  192.168.0.253  192.168.0.2
!当 R2624-A 恢复正常，R2624-A 路由器 VRRP 状态变化
```

任务 6.2　大型（单核心）网络综合项目

情境回顾：某大企业集团为了加快集团的信息化建设，需要将现有的企业各子网络进行升级更新，将企业网建设成以集团办公自动化、电子商务、业务综合管理、多媒体视频会议、远程通信、信息发布及查询为核心，以现代网络技术为依托，技术先进、扩展性强的大型网络；将集团的各种办公室、多媒体会议室、控制中心的 PC 机、工作站、终端设备、控制系统用高速计算机网络连接起来，实现内、外沟通的现代化计算机网络系统。该网络系统是日后支持办公自动化、供应链管理以及各应用系统运行的基础设施。为了确保这些关键应用系统的正常运行、安全和发展，系统必须具备如下特性：

① 采用先进的网络通信技术，完成集团企业网的建设，实现各分公司的信息化。

② 在整个企业集团内实现所有部门的办公自动化，提高工作效率和管理服务水平。

③ 在整个企业集团内实现资源共享、产品信息共享、实时新闻发布。

④ 在整个企业集团内实现财务电算化。

⑤ 在整个企业集团内实现集中式的供应链管理系统和客户服务关系管理系统。

根据项目需求方提出的以上要求进行分析，首先要根据网络具体情况，合理规划网络，确定出建设后的网络拓扑结构和在更新升级中所用的设备，然后根据设备自身的特性合理地做好相关功能的配置。主要通过以下几个阶段来完成网络的集成。

1. 建设后的网络拓扑

建设后的网络拓扑如图 6-2 所示。

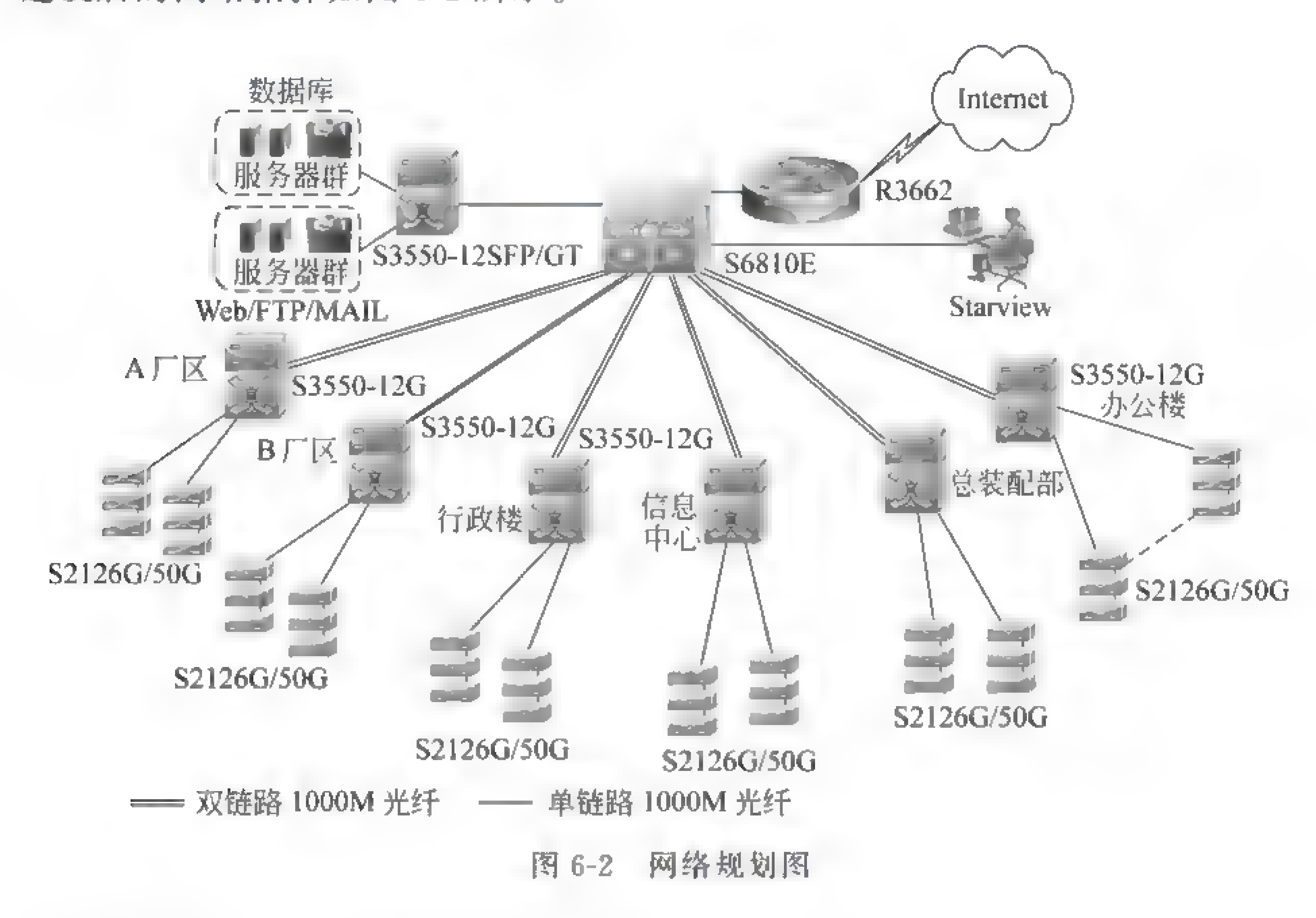


图 6-2　网络规划图

2. 网络实现的功能和网络拓扑的提出

实现内部网络 VLAN 划分，具备三层路由功能，并启用 OSPF 路由协议；病毒攻击防护、出口实现 NAT 地址转换，全网采用 Starview 进行管理。网络拓扑如图 6-3 所示，其中，

① 出口设备：R2624 路由器 1 台；

② 核心设备：S68 系列(或 S65/S35 系列)设备 1 台，配置千兆光纤接口 2 块；

③ 汇聚设备：S3550-24 2 台，每台配置 1 块千兆光纤接口；

④ 接入设备：S2126G 二层交换机 4 台；实验 PC8 台；终端用户的默认网关指向各自对应的 VLAN 接口的 IP 地址。

3. 具体实施步骤

第一步：基本配置。

(1) S2126G-A1 基本配置

```
hostname S2126G-A1
vlan 1
exit
```

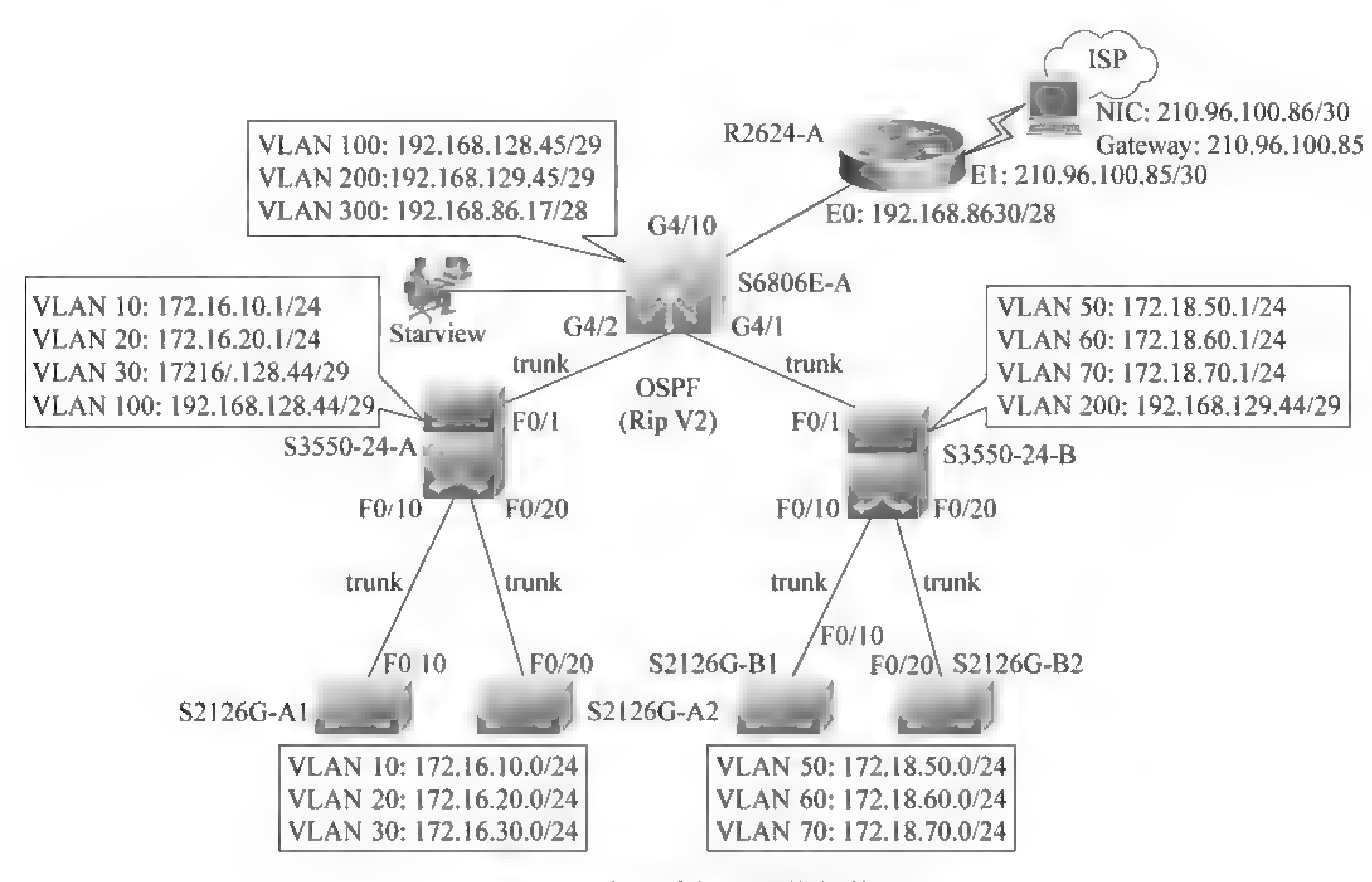


图 6-3　大型单核心网络拓扑图

```
vlan 10                                   !划分 vlan 10
exit
vlan 20                                   !划分 vlan 10
exit
vlan 30                                   !划分 vlan 10
exit
enable secret level 1 0 star              !设置 telnet 密码
enable secret level 15 0 star             !设置特权模式密码
interface range fastEthernet 0/1-3
switchport access vlan 10                 !将 f0/1、f0/2 和 f0/3 划分到 vlan 10 里
exit
interface range fastEthernet 0/4-6
switchport access vlan 20                 !将 f0/4,f0/5 和 f0/6 划分到 vlan 20 里
exit
interface range fastEthernet 0/7-9
switchport access vlan 30                 !将 f0/7,f0/8 和 f0/9 划分到 vlan 30 里
exit
interface fastEthernet 0/10
switchport mode trunk                     !将 f0/10 设置为 trunk 模式
exit
end
S2126G-A1#
```

(2) S2126G-A2 基本配置

```
hostname S2126G-A2
vlan 1
```

```
exit
vlan 10
exit
vlan 20
exit
vlan 30
exit
enable secret level 1 0 star
enable secret level 15 0 star
interface range fastEthernet 0/1-3
switchport access vlan 10
exit
interface range fastEthernet 0/4-6
switchport access vlan 20
exit
interface range fastEthernet 0/7-9
switchport access vlan 30
exit
interface fastEthernet 0/20
switchport mode trunk
exit
end
S2126G-A2#
```

（3）S2126G-B1 基本配置

```
hostname S2126G-B1
vlan 1
exit
vlan 50
exit
vlan 60
exit
vlan 70
exit
enable secret level 1 0 star
enable secret level 15 0 star
interface range fastEthernet 0/1-3
switchport access vlan 50
exit
interface range fastEthernet 0/4-6
switchport access vlan 60
exit
interface range fastEthernet 0/7-9
switchport access vlan 70
exit
interface fastEthernet 0/10
switchport mode trunk
exit
```

(4) S2126G-B2 基本配置

```
hostname S2126G-B2
vlan 1
exit
vlan 50
exit
vlan 60
exit
vlan 70
exit
enable secret level 1 0 star
enable secret level 15 0 star
interface range fastEthernet 0/1-3
switchport access vlan 50
exit
interface range fastEthernet 0/4-6
switchport access vlan 60
exit
interface range fastEthernet 0/7-9
switchport access vlan 70
exit
interface fastEthernet 0/20
switchport mode trunk
exit
```

(5) S3550-24-A 基本配置

```
hostname S3550-24-A
vlan 1
exit
vlan 10
exit
vlan 20
exit
vlan 30
exit
vlan 100
exit
interface FastEthernet 0/1
switchport mode trunk
exit
interface FastEthernet 0/10
switchport mode trunk
exit
interface FastEthernet 0/20
switchport mode trunk
exit
interface Vlan 1
ip address 192.168.0.1 255.255.255.0
```

```
no shut
exit
!为交换机分配管理 ip 地址
interface Vlan 10
ip address 172.16.10.1 255.255.255.0
no shut
exit
!为 vlan10 分配 ip 地址
interface Vlan 20
ip address 172.16.20.1 255.255.255.0
no shut
exit
!为 vlan20 分配 ip 地址
interface Vlan 30
ip address 172.16.30.1 255.255.255.0
no shut
exit
!为 vlan30 分配 ip 地址
interface Vlan 100
ip address 192.168.128.44 255.255.255.248
no shut
exit
!为 vlan30 分配 ip 地址
```

(6) S3550-24-B 基本配置

```
hostname S3550-24-B
vlan 1
exit
vlan 50
exit
vlan 60
exit
vlan 70
exit
vlan 200
exit
enable secret level 1 0 star
enable secret level 15 0 star
interface FastEthernet 0/1
switchport mode trunk
exit
interface FastEthernet 0/10
switchport mode trunk
exit
interface FastEthernet 0/20
switchport mode trunk
exit
interface Vlan 1
ip address 192.168.0.2 255.255.255.0
```

```
no shut
exit
interface Vlan 50
ip address 172.18.50.1 255.255.255.0
no shut
exit
interface Vlan 60
ip address 172.18.60.1 255.255.255.0
no shut
exit
interface Vlan 70
ip address 172.18.70.1 255.255.255.0
no shut
exit
interface Vlan 200
ip address 192.168.129.44 255.255.255.248
no shut
exit
end
```

(7) S6806E-A 基本配置

```
hostname S6806E-A
enable secret level 1 0 star
enable secret level 15 0 star
interface GigabitEthernet 4/1
switchport mode trunk
exit
interface GigabitEthernet 4/2
switchport mode trunk
exit
interface GigabitEthernet 4/10
switchport access vlan 300
exit
interface Vlan 1
ip address 192.168.0.3 255.255.255.0
no shut
exit
interface Vlan 100
ip address 192.168.128.45 255.255.255.248
no shut
exit
interface Vlan 200
ip address 192.168.129.45 255.255.255.248
no shut
exit
interface Vlan 300
ip address 192.168.86.17 255.255.255.240
no shut
exit
```

```
end
```

(8) R2624-A 基本配置

```
hostname R2624-A
enable password star
interface FastEthernet0
ip address 192.168.86.30 255.255.255.240
no shut
ip nat inside
exit
interface FastEthernet1
ip address 210.96.100.85 255.255.255.252
no shut
ip nat outside
exit
line con 0
line aux 0
line vty 0 4
password star
login
end
```

第二步：OSPF 路由选择协议配置及测试。

(1) S3550-24-A OSPF 路由协议配置

```
router ospf                              !在路由器上启动 OSPF 进程
area 0.0.0.0
network 172.16.10.0 255.255.255.0 area 0.0.0.0
                                         !指定参与交换 ospf 更新的网络以及这些网络所属的区域
network 172.16.20.0 255.255.255.0 area 0.0.0.0
                                         !指定参与交换 ospf 更新的网络以及这些网络所属的区域
network 172.16.30.0 255.255.255.0 area 0.0.0.0
                                         !指定参与交换 ospf 更新的网络以及这些网络所属的区域
network 192.168.128.40 255.255.255.248 area 0.0.0.0
                                         !指定参与交换 ospf 更新的网络以及这些网络所属的区域
end
```

(2) S3550-24-B OSPF 路由协议配置

```
router ospf
area 0.0.0.0
network 172.18.50.0 255.255.255.0 area 0.0.0.0
network 172.18.60.0 255.255.255.0 area 0.0.0.0
network 172.18.70.0 255.255.255.0 area 0.0.0.0
network 192.168.129.40 255.255.255.248 area 0.0.0.0
end
```

(3) S6806E OSPF 路由协议配置

```
router ospf
```

```
area 0.0.0.0
network 192.168.86.16 255.255.255.240 area 0.0.0.0
network 192.168.128.40 255.255.255.248 area 0.0.0.0
network 192.168.129.40 255.255.255.248 area 0.0.0.0
end
```

(4) R2624-A OSPF 路由协议配置

```
router ospf 1                  !启动 ospf 进程并指定本地进程号
network 210.96.100.84 0.0.0.3 area 0.0.0.0
network 192.168.86.16 0.0.0.15 area 0.0.0.0
default-information originate always
                               !不管路由器是否存在默认路由，总是向其他路由器公告默认路由
end
```

(5) OSPF 验证

① 查看 S3550-24-A 路由表及相关信息

```
S3550-24-A# show ip route          !以下路由信息除了直连路由外，都是通过 ospf 学习来的

Type:  C - connected,S - static,R - RIP,O - OSPF,IA - OSPF inter area
       N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1,E2 - OSPF external type 2
Type Destination IP    Next hop      Interface Distance Metric  Status
-----------------------------------------------------------------------
O    E2 0.0.0.0/0       192.168.128.45   VL100     110     1     Active
C    172.16.10.0/24     0.0.0.0          VL10      0       0     Active
C    172.16.20.0/24     0.0.0.0          VL20      0       0     Active
C    172.16.30.0/24     0.0.0.0          VL30      0       0     Active
O    172.18.50.0/24     192.168.128.45   VL100     110     3     Active
O    172.18.60.0/24     192.168.128.45   VL100     110     3     Active
O    172.18.70.0/24     192.168.128.45   VL100     110     3     Active
C    192.168.0.0/24     0.0.0.0          VL1       0       0     Active
O    192.168.86.16/28   192.168.128.45   VL100     110     2     Active
C    192.168.128.40/29  0.0.0.0          VL1000    0       0     Active
O    192.168.129.40/29  192.168.128.45   VL100     110     2     Active
O    210.96.100.84/30   192.168.128.45   VL100     110     3     Active
S3550-24-A# show ip ospf neighbor       !查看 S3550-24-A 的邻居路由器
Neighbor ID     Pri State       DeadTime Address        Interface
-----------------------------------------------------------------------
192.168.129.45  1   full/DR       00:00:32  192.168.128.45  VL100
S3550-24-A#
```

② 查看 S3550-24-B 路由表及相关信息

```
S3550-24-B# show ip route          !以下路由信息除了直连路由外，都是通过 ospf 学习来的
Type: C- connected,S- static,R- RIP,O- OSPF,IA- OSPF inter area
     N1- OSPF NSSA external type 1,N2- OSPF NSSA external type 2
     E1- OSPF external type 1,E2  OSPF external type 2
Type Destination IP    Next hop      Interface Distance Metric    Status
```

```
O       E2 0.0.0.0/0       192.168.129.45     VL200      110      1        Active
O       172.16.10.0/24     192.168.129.45     VL200      110      3        Active
O       172.16.20.0/24     192.168.129.45     VL200      110      3        Active
O       172.16.30.0/24     192.168.129.45     VL200      110      3        Active
C       172.18.50.0/24     0.0.0.0            VL50       0        0        Active
C       172.18.60.0/24     0.0.0.0            VL60       0        0        Active
C       172.18.70.0/24     0.0.0.0            VL70       0        0        Active
C       192.168.0.0/24     0.0.0.0            VL1        0        0        Active
O       192.168.86.16/28   192.168.129.45     VL200      110      2        Active
O       192.168.128.40/29  192.168.129.45     VL200      110      2        Active
C       192.168.129.40/29  0.0.0.0            VL200      0        0        Active
O       210.96.100.84/30   192.168.129.45     VL200      110      3        Active
S3550-24-B# show ip ospf neighbor          !查看 S3550-24-B 的邻居路由器。

Neighbor ID     Pri State          DeadTime Address        Interface
--------------------------------------------------------------------
192.168.129.45   1   full/DR          00:00:35 192.168.129.45 VL200
```

③ 查看 S6806E-A 路由表及相关信息

```
S6806E-A# show ip route        !以下路由信息除了直连路由外，都是通过 ospf 学习来的
Type: C - connected,S - static,R - RIP,B - BGP,P - policy
      O - OSPF,IA - OSPF inter area
      N1 - OSPF NSSA external type 1,N2 - OSPF NSSA external type 2
      E1 - OSPF external type 1,E2 - OSPF external type 2
Type Destination IP     Next hop        Interface Distance Metric  Status
--------------------------------------------------------------------
O       E2 0.0.0.0/0       192.168.86.30      VL300     110     1     Active
O       172.16.10.0/24     192.168.128.44     VL100     110     2     Active
O       172.16.20.0/24     192.168.128.44     VL100     110     2     Active
O       172.16.30.0/24     192.168.128.44     VL100     110     2     Active
O       172.18.50.0/24     192.168.129.44     VL200     110     2     Active
O       172.18.60.0/24     192.168.129.44     VL200     110     2     Active
O       172.18.70.0/24     192.168.129.44     VL200     110     2     Active
C       192.168.0.0/24     0.0.0.0            VL1       0       0     Active
C       192.168.86.16/28   0.0.0.0            VL300     0       0     Active
C       192.168.128.40/29  0.0.0.0            VL100     0       0     Active
C       192.168.129.40/29  0.0.0.0            VL200     0       0     Active
O       210.96.100.84/30   192.168.86.30      VL300     110     2     Active
S6806E-A# show ip ospf neighbor             !查看 S6806E-A 的 ospf 邻居
Neighbor ID     Pri State          DeadTime Address         Interface

210.96.100.85   1   full/BDR     00:00:31 192.168.86.30   VL300
192.168.128.44   1   full/BDR     00:00:30 192.168.128.44   VL100
192.168.129.44   1   full/BDR     00:00:37 192.168.129.44   VL200
S6806E-A#
```

④ 查看 R2624 A 路由表及相关信息

```
R2624 A# show ip route
```

```
Codes: C - connected,S - static, R - RIP
       O - OSPF,IA - OSPF inter area
       E1 - OSPF external type 1,E2 - OSPF external type 2
Gateway of last resort is 210.96.100.86 to network 0.0.0.0
       192.168.86.0/28 is subnetted,1 subnets
C      192.168.86.16 is directly connected,FastEthernet0
       172.16.0.0/24 is subnetted,3 subnets
O      172.16.30.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
O      172.16.20.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
O      172.16.10.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
       172.18.0.0/24 is subnetted,3 subnets
O      172.18.60.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
O      172.18.50.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
O      172.18.70.0 [110/3] via 192.168.86.17,00:43:05,FastEthernet0
       210.96.100.0/30 is subnetted,1 subnets
C      210.96.100.84 is directly connected,FastEthernet1
       192.168.128.0/29 is subnetted,1 subnets
O      192.168.128.40 [110/2] via 192.168.86.17,00:43:05,FastEthernet0
       192.168.129.0/29 is subnetted,1 subnets
O      192.168.129.40 [110/2] via 192.168.86.17,00:43:05,FastEthernet0
S*     0.0.0.0/0 [1/0] via 210.96.100.86
R2624-A# show ip ospf neighbor          !查看 R2624-A 的 ospf 邻居
Neighbor ID   Pri     State     Dead Time     Address        Interface
----------------------------------------------------------------------
192.168.129.45   1  FULL/DR   00:00:36   192.168.86.17   FastEthernet0
R2624-A#
```

第三步：基本连通性测试，包括网络连通性测试和不同 VLAN 间用户通信连通性测试。

(1) 网络连通性测试

对于在 S2126G-A1 的 vlan 10 内的用户，用户主机 IP 地址为 172.16.10.195/24，网关为 172.16.10.1。

```
D:\>ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix .:
        IP Address.....................  : 172.16.10.195
        Subnet Mask....................  : 255.255.255.0
        Default Gateway................  : 172.16.10.1
!在 vlan10 里,ip 地址为 172.16.10.195 主机为测试主机
D:\>ping 172.16.10.1
Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time<10ms TTL=64
Reply from 172.16.10.1: bytes=32 time<10ms TTL=64
!测试到网关的连通性
D:\>ping 172.16.20.1
Pinging 172.16.20.1 with 32 bytes of data:
Reply from 172.16.20.1: bytes=32 time<10ms TTL=64
```

```
!测试到 S3550-24-A vlan 20 svi 口的连通性
D:\>ping 172.16.30.1
Pinging 172.16.30.1 with 32 bytes of data:
Reply from 172.16.30.1: bytes=32 time<10ms TTL=64
!测试到 S3550-24-A vlan 30 svi 口的连通性
D:\>ping 192.168.128.44
Pinging 192.168.128.44 with 32 bytes of data:
Reply from 192.168.128.44: bytes=32 time<10ms TTL=64
!测试到 S3550-24-A vlan 100 svi 口的连通性
D:\>ping 192.168.128.45
Pinging 192.168.128.45 with 32 bytes of data:
Reply from 192.168.128.45: bytes=32 time=2ms TTL=62
!测试到 S6806E-A vlan 100 的 svi 口的连通性
D:\>ping 192.168.129.45
Pinging 192.168.129.45 with 32 bytes of data:
Reply from 192.168.129.45: bytes=32 time=1ms TTL=63
!测试到 S6806E-A vlan 200 的 svi 口的连通性
D:\>ping 192.168.86.17
Pinging 192.168.86.17 with 32 bytes of data:
Reply from 192.168.86.17: bytes=32 time=1ms TTL=63
!测试到 S6806E-A vlan 300 的 svi 口的连通性
D:\>ping 192.168.86.30
Pinging 192.168.86.30 with 32 bytes of data:
Reply from 192.168.86.30: bytes=32 time<10ms TTL=253
!测试到 R2624-A f0 口的连通性
D:\>ping 172.18.50.1
Pinging 172.18.50.1 with 32 bytes of data:
Reply from 172.18.50.1: bytes=32 time=1ms TTL=62
Reply from 172.18.50.1: bytes=32 time=2ms TTL=62
!测试到 S3550-24-B vlan 50 的 svi 口的连通性
D:\>ping 172.18.60.1
Pinging 172.18.60.1 with 32 bytes of data:
Reply from 172.18.60.1: bytes=32 time=1ms TTL=62
!测试到 S3550-24-B vlan 60 的 svi 口的连通性
D:\>ping 172.18.70.1
Pinging 172.18.70.1 with 32 bytes of data:
Reply from 172.18.70.1: bytes=32 time=1ms TTL=62
!测试到 S3550-24-B vlan 70 的 svi 口的连通性
D:\>ping 192.168.129.44
Pinging 192.168.129.44 with 32 bytes of data:
Reply from 192.168.129.44: bytes=32 time<10ms TTL=62
!测试到 S3550-24-B vlan 200 的 svi 口的连通性
D:\>ping 210.96.100.85
Pinging 210.96.100.85 with 32 bytes of data:
Reply from 210.96.100.85: bytes=32 time=1ms TTL=253
!测试到 R2624-A 路由器 F1 口的连通性
```

(2) VLAN 间通信测试

这里只举例测试 vlan 50 里用户 172.18.50.195 与 vlan 10 里用户 172.16.10.179 通

信的连通性，其中主机指向各自的网关。由于不同 VLAN 间的用户通信测试方法相同，这里将举例说明。

```
D:\> ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix .:
        IP Address.......................  : 172.18.50.195
        Subnet Mask.....................  : 255.255.255.0
        Default Gateway..............  : 172.18.50.1
D:\>ping 172.18.50.1
Pinging 172.18.50.1 with 32 bytes of data:
Reply from 172.18.50.1: bytes=32 time<10ms TTL=64
!vlan 50 用户 172.18.50.195 测试到此网关的连通性
D:\>ping 192.168.86.30
Pinging 192.168.86.30 with 32 bytes of data:
Reply from 192.168.86.30: bytes=32 time<10ms TTL=253
!测试到网络的连通性
D:\>ping 172.16.10.179
Pinging 172.16.10.179 with 32 bytes of data:
Reply from 172.16.10.179: bytes=32 time<10ms TTL=125
Reply from 172.16.10.179: bytes=32 time<10ms TTL=125
Reply from 172.16.10.179: bytes=32 time<10ms TTL=125
Reply from 172.16.10.179: bytes=32 time<10ms TTL=125
!测试 vlan50 用户 172.18.50.195 到 vlan10 用户 172.16.10.179 的连通性
```

第四步：NAT 功能配置及测试。NAT 功能是在 R2624-A 上实现的。

(1) 在 R2624-A 上配置 NAT 功能。

```
access-list 10 permit any
exit
ip nat inside source list 10 interface FastEthernet1 overload
interface FastEthernet0
ip nat inside
exit
interface FastEthernet1
ip nat outside
exit
```

(2) 测试 nat 功能。如拓扑图所示，在 R2624 A F1 口的对端放置 PC 模拟 ISP。通过内部主机 172.18.50.195 ping 主机 210.96.100.86，在路由器上调试 NAT，通过查看相关调试信息测试 NAT 功能。

```
R2624-A# debug ip nat
NAT events debugging is on
R2624-A# debug ip nat detailed
NAT detailed events debugging is on
R2624 A# debug ip nat packet
NAT packet flow events debugging is on
```

```
R2624-A#
!在 R2624-A 上开启 NAT debug 功能
D:\Documents and Settings\Administrator> ipconfig
Windows 2000 IP Configuration
Ethernet adapter 本地连接:
        Connection-specific DNS Suffix.:
        IP Address......................  : 172.18.50.195
        Subnet Mask.....................  : 255.255.255.0
        Default Gateway.................  : 172.18.50.1
D:\ > ping 210.96.100.86
!客户机访问外部网络主机
Pinging 210.96.100.86 with 32 bytes of data:
Reply from 210.96.100.86: bytes=32 time=3ms TTL=125
Reply from 210.96.100.86: bytes=32 time=3ms TTL=125
Reply from 210.96.100.86: bytes=32 time=3ms TTL=125
2624-A#
IPNAT: I* icmp 210.96.100.85:512->210.96.100.86:512 [5930, 60]
IPNAT: O icmp 210.96.100.86:512->210.96.100.85:512 [21452, 60]
IPNAT: O* icmp 210.96.100.86:512->172.18.50.195:512 [21452, 60]
IPNAT: I icmp 172.18.50.195:512->210.96.100.86:512 [5931, 60]
IPNAT: I* icmp 210.96.100.85:512->210.96.100.86:512 [5931, 60]
IPNAT: O icmp 210.96.100.86:512->210.96.100.85:512 [21453, 60]
IPNAT: O* icmp 210.96.100.86:512->172.18.50.195:512 [21453, 60]
!NAT 相关信息,可以看到 NAT 成功
```

规律总结(检查)

任何规划都是从需求开始的,网络规划也不例外。马斯洛的需求理论中提到:生理需求是其他所有需求的基础需求,在人们转向较高层次的需求之前,总是尽力先满足这类需求,一个人在饥饿时不会对其他任何事物感兴趣。如果拿马斯洛的理论类比网络需求及规划,生理需求可以看做带宽需求,更高层次的需求可以比作业务应用。10 年前,在带宽资源有限的情况下,任何企业都不敢想象基于 IP 网络的视频会议应用,而如今随着技术的进步,带宽不再是瓶颈,企业把需求转向能为自身带来更多利益的、更加切合实际的业务应用上。

我们在以上任务中体现的主要还是基础网络的规划和构建,随着技术的发展,不仅仅是视频应用、VoIP、即时通信、数据存储、无线通信、安全中心等基于 IP 网络的业务应用不再遥不可及。事实上,两年前,中国企业的 IT 业务应用已经呈现多元化的趋势,未来基于 IP 网络的业务应用会越来越多。

当基于 IP 网络多元化的业务应用给企业带来便利的同时,也给企业带来不小的难题,那就是如何管理。2007 年,经过抽样调查发现,有 83%网管人员每日疲于奔波在解决各种应用问题上,他们更愿意将时间用于优化网络。此外,在调查中发现,能够实现对安全、性能、故障、配置和资产进行综合管理的平台成为企业网络构建中考虑的重要因素。

中国企业网络建设及规划经过几年的发展,已经有了长足的进步。企业不再对自己的需求茫然无措。如何通过 IP 网络提升业务运转能力,减少网络运营成本,获取更大的

利润，已经成为企业明确而清晰的需求，但问题是，有了需求不知道怎么落实，很多企业急需找到适合自身的网络解决方案。

针对单一设备的网络解决方案早已一去不返了。由于业务呈现的多元化趋势，企业需要的是全面的、统一的、易于管理的整体 IT 网络解决方案。对于 IP 业务应用的承载体，需要网络数据通信解决方案；对于移动接入用户，需要无线通信解决方案；对于海量数据，需要 IP 存储解决方案；为了保障业务不受外来威胁影响，需要网络安全解决方案。以 Cisco、华为、锐捷为代表的厂家，都能够同时提供这些产品和整体技术解决方案。

拓展提高（拓展）

1. R2624-A 参考配置

```
R2624-A(config)#end
R2624-A#show run
Building configuration...
Current configuration:
version 6.14(2)
hostname "R2624-A"
enable password star
ip subnet-zero
interface FastEthernet0
 ip address 192.168.86.30 255.255.255.240
 ip nat inside
!
interface FastEthernet1
 ip address 210.96.100.85 255.255.255.252
 ip nat outside
interface FastEthernet2
no ip address
shutdown
interface FastEthernet3
no ip address
shutdown
interface Serial0
no ip address
interface Serial1
no ip address
router ospf 1
network 210.96.100.84 0.0.0.3 area 0.0.0.0
network 192.168.86.16 0.0.0.15 area 0.0.0.0
default-information originate always
ip nat inside source list 10 interface FastEthernet1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 210.96.100.86
access-list 10 permit any
line con 0
line aux 0
```

```
line vty 0 4
password star
login
end
```

2. S6806E-A 参考配置

```
S6806E-A# show run
System software version: 2.41(2) Build Sep 19 2005 Rel
Building configuration...
Current configuration: 883 bytes
version 1.0
install 4 12sfp/gt
ip routing algorithm CRC32_UPPER
hostname S6806E-A
enable secret level 1 5 $2IOrJ%(3LMp]K* .4AxB^"[/QwNq&# Z1
enable secret level 15 5 $2knAxB^3glowNq&4h'@ IOrJQimLMp]K
interface GigabitEthernet 4/1
switchport mode trunk
interface GigabitEthernet 4/2
switchport mode trunk
interface GigabitEthernet 4/10
switchport access vlan 300
interface Vlan 1
ip address 192.168.0.3 255.255.255.0
interface Vlan 100
ip address 192.168.128.45 255.255.255.248
interface Vlan 200
ip address 192.168.129.45 255.255.255.248
interface Vlan 300
ip address 192.168.86.17 255.255.255.240
router ospf
area 0.0.0.0
network 192.168.86.16 255.255.255.240 area 0.0.0.0
network 192.168.128.40 255.255.255.248 area 0.0.0.0
network 192.168.129.40 255.255.255.248 area 0.0.0.0
snmp-server community star ro
end
```

3. S3550-24-B 参考配置

```
S3550-24-B# show run
Building configuration...
Current configuration: 968 bytes
version 1.0
hostname S3550-24 B
vlan 1
vlan 50
vlan 60
```

```
vlan 70
vlan 200
enable secret level 1 5 $2qkE,lu3dhl&-8U4ein'.tjQfjo+/7R
enable secret level 15 5 $2G1X)sv3>H.Y*T74C,tZ[V/QD+S(\W&
interface FastEthernet 0/1
switchport mode trunk
interface FastEthernet 0/10
switchport mode trunk
interface FastEthernet 0/20
switchport mode trunk
interface Vlan 1
ip address 192.168.0.2 255.255.255.0
interface Vlan 50
ip address 172.18.50.1 255.255.255.0
interface Vlan 60
ip address 172.18.60.1 255.255.255.0
interface Vlan 70
ip address 172.18.70.1 255.255.255.0
interface Vlan 200
ip address 192.168.129.44 255.255.255.248
router ospf
area 0.0.0.0
network 172.18.50.0 255.255.255.0 area 0.0.0.0
network 172.18.60.0 255.255.255.0 area 0.0.0.0
network 172.18.70.0 255.255.255.0 area 0.0.0.0
network 192.168.129.40 255.255.255.248 area 0.0.0.0
snmp-server community star rw
end
```

4. S3550-24-A 参考配置

```
S3550-24-A# show run
Building configuration...
Current configuration: 968 bytes
version 1.0
hostname S3550-24-A
vlan 1
vlan 10
vlan 20
vlan 30
vlan 100
enable secret level 15 0 100
enable secret level 15 5 100
interface FastEthernet 0/1
switchport mode trunk
interface FastEthernet 0/10
switchport mode trunk
interface FastEthernet 0/20
switchport mode trunk
```

```
interface Vlan 1
ip address 192.168.0.1 255.255.255.0
interface Vlan 10
ip address 172.16.10.1 255.255.255.0
interface Vlan 20
ip address 172.16.20.1 255.255.255.0
interface Vlan 30
ip address 172.16.30.1 255.255.255.0
interface Vlan 100
ip address 192.168.128.44 255.255.255.248
router ospf
area 0.0.0.0
network 172.16.10.0 255.255.255.0 area 0.0.0.0
network 172.16.20.0 255.255.255.0 area 0.0.0.0
network 172.16.30.0 255.255.255.0 area 0.0.0.0
network 192.168.128.40 255.255.255.248 area 0.0.0.0
snmp-server community star rw
end
```

5. S2126G-B1 参考配置

```
S2126G-B1# show run
System software version: 1.61 Build Jun 17 2005 Release
Building configuration...
Current configuration: 800 bytes
version 1.0
hostname S2126G-B1
vlan 1
vlan 50
vlan 60
vlan 70
enable secret level 15 0 100
enable secret level 15 5 100
interface fastEthernet 0/1
switchport access vlan 50
interface fastEthernet 0/2
switchport access vlan 50
interface fastEthernet 0/3
switchport access vlan 50
interface fastEthernet 0/4
switchport access vlan 60
interface fastEthernet 0/5
switchport access vlan 60
interface fastEthernet 0/6
switchport access vlan 60
interface fastEthernet 0/7
switchport access vlan 70
interface fastEthernet 0/8
switchport access vlan 70
```

```
interface fastEthernet 0/9
switchport access vlan 70
interface fastEthernet 0/10
switchport mode trunk
end
S2126G-B1#
```

6. S2126G-B2 参考配置

```
S2126G-B2# show run
System software version: 1.61 Build Jun 17 2005 Release
Building configuration...
Current configuration: 800 bytes
version 1.0
hostname S2126G-B2
vlan 1
vlan 50
vlan 60
!
vlan 70
enable secret level 1 5 $29=G1X)3R:>H.Y* 4_;C,tZ[Q0<D+S(\
enable secret level 15 5 $2Y* T7+ .3tZ[V/,|4S(\W&-/QX)sv'~ 1
interface fastEthernet 0/1
switchport access vlan 50
interface fastEthernet 0/2
switchport access vlan 50
interface fastEthernet 0/3
switchport access vlan 50
interface fastEthernet 0/4
switchport access vlan 60
interface fastEthernet 0/5
switchport access vlan 60
interface fastEthernet 0/6
switchport access vlan 60
interface fastEthernet 0/7
switchport access vlan 70
interface fastEthernet 0/8
switchport access vlan 70
interface fastEthernet 0/9
switchport access vlan 70
interface fastEthernet 0/10
switchport mode trunk
end
S2126G-B2#
```

7. S2126G-A1 参考配置

```
S2126G-A1# show run
Building configuration...
```

```
Current configuration: 800 bytes
version 1.0
hostname S2126G-A1
vlan 1
vlan 10
vlan 20
vlan 30
enable secret level 1 5 $2@ IOrJ%3mLMp]K* 4nAxB^"[QowNq&# Z
enable secret level 15 5 $2-/-aeh3'~ 1'dfi4+.t{bckQ,|7zygl
interface fastEthernet 0/1
switchport access vlan 10
interface fastEthernet 0/2
switchport access vlan 10
interface fastEthernet 0/3
switchport access vlan 10
interface fastEthernet 0/4
switchport access vlan 20
interface fastEthernet 0/5
switchport access vlan 20
interface fastEthernet 0/6
switchport access vlan 20
interface fastEthernet 0/7
switchport access vlan 30
interface fastEthernet 0/8
switchport access vlan 30
interface fastEthernet 0/9
switchport access vlan 30
interface fastEthernet 0/10
switchport mode trunk
end
S2126G-A1#
```

8. S2126G-A2 参考配置

```
S2126G-A1# show run
Building configuration...
Current configuration: 800 bytes
version 1.0
hostname S2126G-A2
vlan 1
vlan 10
vlan 20
vlan 30
enable secret level 1 5 $2@ IOrJ%3mLMp]K* 4nAxB^"[QowNq&# Z
enable secret level 15 5 $2-/-aeh3'~ 1'dfi4+.t{bckQ,|7zygl
interface fastEthernet 0/1
switchport access vlan 10
interface fastEthernet 0/2
switchport access vlan 10
```

```
interface fastEthernet 0/3
switchport access vlan 10
interface fastEthernet 0/4
switchport access vlan 20
interface fastEthernet 0/5
switchport access vlan 20
interface fastEthernet 0/6
switchport access vlan 20
interface fastEthernet 0/7
switchport access vlan 30
interface fastEthernet 0/8
switchport access vlan 30
interface fastEthernet 0/9
switchport access vlan 30
interface fastEthernet 0/10
switchport mode trunk
end
S2126G-A2#
```

参 考 文 献

1. 张国清.网络设备配置与调试项目实训.北京：清华大学出版社，2008
2. [美]Cisco System 公司.思科网络技术学院教程.北京：人民邮电出版社，2004
3. 王劲松，苗玲等.Cisco 路由器实用技术.北京：中国铁道出版社，2006
4. 电子行业职业技能鉴定指导中心组编.网络设备安装与调试.北京：电子工业出版社，2009
5. 蔡学军.网络互联技术.北京：高等教育出版社，2004
6. 刘鲁川，王小斌等.Cisco Cataly 系列交换机的使用与组网技术.北京：清华大学出版社，2002